adam13zajac@gmail.com

Biblioteczka **Komputer Świat**



DVD I KŚ+
30 PRZYDATNYCH PROGRAMÓW DO OCHRONY PRYWATNOŚCI W SIECI

ISO płyty do pobrania z ksplus.pl

ZADBAJ O SWOJĄ

PRYWATNOŚĆ I ANONIMOWOŚĆ

NA KOMPUTERZE, SMARTFONIE, W SIECI

Z TEJ KSIĄŻKI DOWIESZ SIĘ, JAK:

- bronić się przed szpiegowaniem na komputerze i smartfonie
- usuwać ślady z dysku i sieci
- szyfrować system
- namierzyć smartfon
- korzystać z bezpiecznego e-maila i komunikatora
- anonimowo przeglądać internet
- łączyć się przez Tor i VPN

adam13zajac@gmail.com



Z TĄ KSIĄŻKĄ E-WYDANIE GRATIS

Poniżej znajduje się płyta z kodem bonusowym dającym dostęp do e-wydania tej książki w serwisie KŚ+ (ksplus.pl) oraz pliku ISO z cyfrową wersją płyty do pobrania.

NA PŁYCIE DVD

Płyta dołączona do tej książki zawiera 30 najlepszych darmowych narzędzi do ochrony prywatności i zachowania anonimowości w internecie.

Jeżeli brakuje płyty, poinformuj sprzedawcę lub redakcję: pomoc@komputerswiat.pl

Fot. ValeryBrozhinsky/iStockphoto.com.com

OCHRONA PRYWATNOŚCI

30 NAJLEPSZYCH NARZĘDZI

PŁYTA JEST DODATKIEM DO KSIĄŻKI KOMPUTER ŚWIAT BIBLIOTECZKA 2|2022

Biblioteczka Komputer Świat

NA PŁYCIE ZNAJDZIESZ KOD DO E-WYDANIA I CYFROWEJ WERSJI PŁYTY W KSPLUS.PL

Kod bonusowy należy zarejestrować w KŚ+ (ksplus.pl)

adam13zajac@gmail.com

Biblioteczka Komputer Świat

KRZYSZTOF DZIEDZIC

PRYWATNOŚĆ I ANONIMOWOŚĆ

NA KOMPUTERZE, SMARTFONIE, W SIECI

ringier axel springer

adam13zajac@gmail.com

AUTOR: Krzysztof Dziedzic

REDAKTORZY PROWADZĄCY: Rafał Kamiński, Agnieszka Al-Jawahiri

PRZYGOTOWANIE PŁYTY: Mariusz Michalski

PROJEKT OKŁADKI: Robert Dobrzyński

SKŁAD I ŁAMANIE: Mariusz Rybak

KOREKTA: Jolanta Rososińska

WYDAWCA:

RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
02-672 Warszawa, ul. Domaniewska 49
tel. 12 2600200 (BOK)
www.ringieraxelspringer.pl

ISBN 978-83-8250-139-1

© Copyright by Ringier Axel Springer Polska Sp. z o.o.

Warszawa 2022

BUSINESS PROJECT MANAGER: Paweł Bulwan

DRUK I OPRAWA:
Drukarnia im. Adama Półtawskiego, Kielce

EGZEMPLARZE ARCHIWALNE:
literia.pl, prenumerata.axel@qg.com

E-WYDANIA, E-PRENUMERATA:
ksplus.pl

KONTAKT:
redakcja@komputerswiat.pl

INTERNET:
komputerswiat.pl, ksplus.pl

Płyta DVD jest dodatkiem do książki

ringier
axel springer

adam13zajac@gmail.com

adam13zajac@gmail.com

1 Anonimowość i prywatność w sieci a nasze bezpieczeństwo

Jesteśmy w sieci przez całą dobę. Nasze smartfony bez przerwy są aktywne i otrzymujemy powiadomienia z mediów społecznościowych. Na komputerze również non stop korzystamy z internetu. Warto się zastanowić, jakie dane i ślady po sobie zostawiamy i czy jest to bezpieczne

Internet oferuje bardzo wiele możliwości. Pozwala szybko nawiązać kontakt z milionami innych użytkowników przez sieci społecznościowe, możemy dokonywać zakupów i udostępniać różnego rodzaju treści. Warto jednak zastanowić się, co się dzieje z naszą prywatnością, gdy na przykład wrzucamy do sieci zdjęcie informujące wszystkich, że jesteśmy na wakacjach. Gdy udostępniamy je publicznie, wszyscy wiedzą, gdzie jesteśmy w danej chwili. Ze względów bezpieczeństwa jest to problem. Z jednej strony wiadomo wtedy, gdzie nas nie ma, co może ułatwić dokonanie włamania. Z drugiej wiadomo też, gdzie jesteśmy i co robimy, co również może pomóc w kradzieży i pozwala wnioskować o naszym stanie posiadania.

Prywatność a internet

Warto pamiętać, że zwykłe przeglądanie internetu niesie ze sobą szereg konsekwencji. Gdy odwiedzamy różne strony czy przechodzimy z witryny do witryny, przypisywane są do nas pliki cookie – ciasteczka. Ciasteczka to elementy pozwalające identyfikować naszą cyfrową tożsamość na wielu witrynach.
Ich zaletą jest to, że pozwalają dostarczać nam odpowiednich treści, niekiedy wręcz warunkują funkcjonowanie spersonalizowanych usług.
A wadą jest to, że niemal automatyczne akceptowanie przez nas ustawień prywatności serwisów oznacza zgodę na personalizowanie treści reklamowych.
W efekcie gdy na przykład rozglądamy się za nowym laptopem, już po krótkim wyszukiwaniu takiego sprzętu, odwiedzając jakikolwiek serwis zawierający reklamy Google AdSense, będziemy widzieć właśnie reklamy laptopów.

Automatyzacja i algorytmy śledzące

Bardzo prężnie rozwija się technologia pozwalająca na automatyczne profilowanie użytkowników. Na podstawie zebranych na ich temat informacji są im przedstawiane takie treści, które mają sprawić, że z większym

adam13zajac@gmail.com

prawdopodobieństwem kupią dany produkt. Oto przykład, jak to działa. Na jednej stronie wypełniamy ankietę, na przykład by skorzystać z promocji czy wziąć udział w konkursie – podajemy w niej jakieś wydawałoby się mało charakterystyczne dane, jak wiek, płeć, zainteresowania. Następnie na innej stronie kupujemy lot samolotem na wakacje. Potwierdzenie płatności zostanie wysłane na nasz adres e-mail na przykład w usłudze Gmail. A potem automatycznie będziemy dostawać przypomnienia, że zbliża się nasz wylot. Zaczniemy otrzymywać mnóstwo reklam związanych z wyjazdem, a nawet z miejscem docelowym. Oprócz tego, jeżeli algorytm stwierdzi na podstawie historii naszych zakupów i wieku, że raczej nie wydajemy dużych sum, będziemy widywali reklamy poradników turystycznych i gadżetów. Gadżety mog być dodatkowo dopasowane do naszej płci. A jeśli automat oceni, że mamy znacznie zasobniejszy portfel, co też widać w historii zakupów, będziemy otrzymywać reklamy luksusowych hoteli, wypożyczalni samochodów itp. Część użytkowników może stwierdzić, że jest to wygodne, że dzięki takim mechanizmom życie staje się prostsze. Tylko że kosztem tej wygody są nasze prywatne dane kupowane przez korporacje, które starają się sprzedać jak najwięcej swoich produktów.

Anonimowość w sieci

Jeśli zależy nam na tym, aby pozostać anonimowym, musimy pamiętać, aby nie popełniać podstawowych błędów, które łatwo mogą zdradzić naszą tożsamość, nawet jeśli korzystamy z usług VPN, sieci Tor i innych anonimizujących serwisów.



Nie logujemy się do wcześniej założonych kont podczas korzystania z sieci Tor

Każde konto zabezpieczone jest hasłem i wszystkie informacje dotyczące logowania zapisywane są na serwerze. Jeżeli więc zalogujemy się na nasze konto, korzystając z sieci Tor, będzie można powiązać nowy adres IP z nami jako użytkownikiem konta, gdyż tylko my możemy mieć do niego dostęp. A my zyskamy fałszywe poczucie bezpieczeństwa. Jeśli wykonamy inne akcje, mając cały czas ten sam adres IP, będzie można je do nas przypisać. (Więcej o sieci Tor w dalszej części książki).

Google
Zaloguj się
Otwórz Gmaila
Adres e-mail lub telefon
@gmail.com
Nie pamiętasz adresu?
To nie Twój komputer? Aby zalogować się prywatnie, użyj trybu gościa. Dowiedz się więcej
Utwórz konto
Dalej

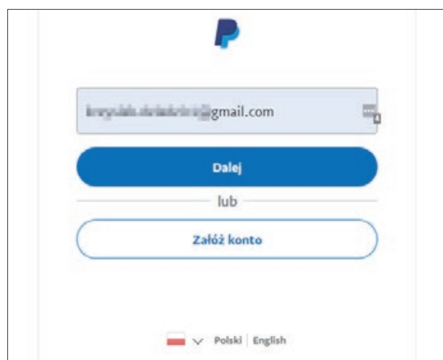


Nie korzystamy z kont, na których mamy dostęp do finansów poprzez sieć Tor

Tego typu konta są jawne dla usługodawców, którzy świadczą nam daną usługę. Musimy być odpowiednio zweryfikowani, zanim otworzymy rachunek bankowy czy potwierdzimy konto PayPal. Dlatego nie ma sensu ukrywać swojej obecności w internecie i jednocześnie logować się do tego typu usług, korzystając z Tora.

Możemy również przysporzyć sobie kłopotów, ponieważ banki w ramach zabezpieczenia mogą blokować konta, do których następują logowania z różnych adresów IP w różnych krajach.

adam13zajac@gmail.com



PRYWATNOŚĆ, BEZPIECZEŃSTWO I ANONIMOWOŚĆ

Zalecenia w tej części książki dotyczą zachowania anonimowości. Jeśli natomiast zależy nam na prywatności i bezpieczeństwie, ale nie na ukrywaniu tożsamości, warto korzystać w czasie logowania na nasze konta z zaszyfrowanego tunelowego połączenia VPN, aby w otwartej sieci nikt nie przechwycił naszych haseł.

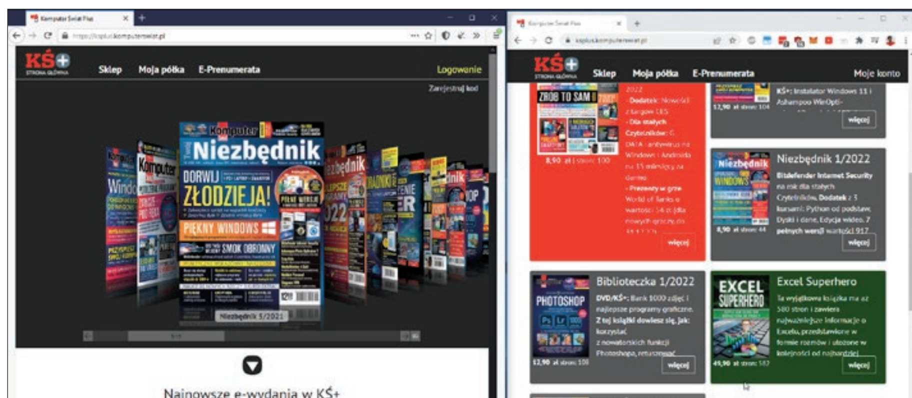
Jeśli więc do weryfikacji konta musieliśmy przesłać skan dowodu lub podawać prywatne dane, nie ma sensu ukrywać się przy próbie logowania.

Nie zmieniamy sieci w trakcie trwania jednej sesji

Jeśli korzystamy z sieci Tor przez na przykład 30 minut i stwierdzimy, że pracuje ona zbyt wolno, a chcemy obejrzeć jakiś materiał, na przykład film, szybciej, nie otwieramy zwykłej przeglądarki i nie przeglądamy zasobów przy jednocześnie aktywnej przeglądarce Tor. Przez takie działanie bardzo łatwo powiązać adresy IP i czasy dostępu do serwerów. Powinniśmy całkowicie zamknąć przeglądarkę Tor i dopiero wtedy korzystać normalnie z internetu. Unikniemy w ten sposób mieszania sieci w ramach jednej sesji.

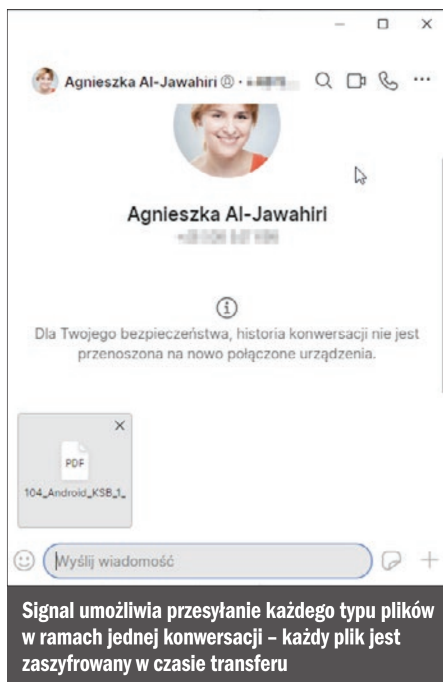
Nie przesyłamy wrażliwych danych bez ich zaszyfrowania

Nie wiemy, kto może nas szpiegować, być może nikt, a być może jakaś zorganizowana grupa. Wszelkiego rodzaju informacje, które są wrażliwe lub szczególnie ważne, nigdy nie powinny być przesyłane przez internet bez wcześniejszego zaszyfrowania. Jeśli nie zamierzamy korzystać ze specjalnych narzędzi do szyfrowania, powinniśmy przynajmniej spakować przesyłane pliki do archiwum i zabezpieczyć je hasłem. Nie jest to



Nie korzystajmy nigdy z przeglądarek anonimowej i zwykłej w tym samym czasie. Umożliwia to zidentyfikowanie nas (Tor Browser po lewej, po prawej Chrome)

adam13zajac@gmail.com

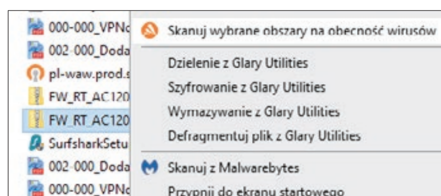


Signal umożliwia przesyłanie każdego typu plików w ramach jednej konwersacji – każdy plik jest zaszyfrowany w czasie transferu

idealne rozwiązanie, ale szybkie, a jeśli ustawimy odpowiednio silne hasło, będzie ono nie do złamania dla zwykłych atakujących. Zaleca się jednak korzystanie z profesjonalnych rozwiązań. Na przykład komunikator Signal umożliwia bezpieczne przesyłanie plików pomiędzy dwoma użytkownikami.

Nie klikamy na podejrzane linki i nie uruchamiamy podejrzanych plików

Otrzymany na przykład w e-mailu link może otwierać prawdziwą stronę internetową, ale może też być to pułapka prowadząca do zainfekowanej witryny, która wykorzystując specjalne skrypty, przechwyci naszą przeglądarkę lub zainstaluje programy typu malware. Podobne zagrożenie zawsze istnieje, gdy otwieramy nieznane pliki, które otrzymaliśmy drogą mailową lub sami pobraliśmy z podejrzanych stron. Wirusy mogą być ukryte nie tylko w aplikacjach, ale również w plikach muzycznych, zdjęciach, dokumentach. Jeżeli zależy nam na ochronie, powinniśmy zainstalować program antywirusowy, który ochroni nas przed tego typu zagrożeniami, gdy przypadkiem otworzymy zły link. Jeśli koniecznie chcemy otworzyć plik pobrany ze źródła, któremu nie całkiem ufamy, warto przeskanować go przed uruchomieniem lub rozpakowaniem. Jeżeli na naszym urządzeniu jest zainstalowane oprogramowanie antywirusowe, najczęściej wystarczy kliknąć na plik prawym przyciskiem myszy i wybrać z menu kontekstowego polecenie **Skanuj**.



Nie udostępniamy prywatnych informacji na nasz temat

Jeżeli zależy nam na anonimowości, nie możemy na stronach internetowych podawać dotyczących nas informacji. Takie dane, jak wiek, data urodzenia, miejsce zamieszkania, ulubione zwierzę, drużyna czy zespół, przezwisko, hobby i inne podobne – z pozoru wydają się mało znaczące. Jednak często, gdy chcemy odzyskać hasło do jakiejś usługi, musimy podać właśnie takie informacje. Jeśli więc opublikujemy je w serwisie społecznościowym lub innym publicznym portalu, atakujący mogą do nich dotrzeć i wykorzystać je, by się pod nas podszyć.

Nie stosujemy słabych haseł

Informacje osobiste mogą także wykorzystywać generatory do łamania haseł. Wystarczy znać kilka podstawowych danych i już można złamać hasło większości mniej doświadczonych użytkowników. Bardzo dużo osób używa jako hasła na przykład swojego imienia i roku urodzenia lub nazwy drużyny piłkarskiej itp. Pamiętajmy, że musimy zabezpieczać nasze konta silnymi hasłami, które nie będą podatne na tego typu

adam13zajac@gmail.com

społecznościowe ataki. Silne hasło powinno mieć przynajmniej 12 znaków, na które składać się będą przynajmniej jedna duża litera, cyfra i znak specjalny. Możemy skorzystać z generatorów haseł, na przykład tego wbudowanego w przeglądarkę Google Chrome.

1 Po uruchomieniu Google Chrome musimy zalogować się na nasz profil (wymagane jest posiadanie konta Google).

2 Otwieramy witrynę, na której chcemy założyć nowe konto, i przechodzimy do formularza rejestracji. Następnie klikamy na pole do wpisywania hasła. Poniżej pojawi się automatycznie wygenerowane silne hasło **A**. Po jego wyborze i zarejestrowaniu konta login razem z hasłem zostanie zapisany w danych przeglądarki.

Zarejestruj się, używając adresu e-mail
Adres e-mail
Imię
Nazwisko
Hasło
Użyj sugerowanego hasła **A** NhCc+3y5yn)Y%y^
Chrome zapisze to hasło na Twoim koncie Google. Nie musisz go pamiętać.
Kraj/region
Polska

3 Za każdym razem przy kliknięciu na pole z hasłem będzie generowane nowe hasło.



Unikamy niepotrzebnego podawania adresu e-mail

Jeśli chcemy założyć konto w jakimś serwisie, żeby uzyskać dostęp do plików lub treści, która nas interesuje, i w tym celu musimy podać e-mail – dobrym rozwiązaniem jest skorzystanie z adresu tymczasowego.
Tego typu adresy można tworzyć bardzo szybko za pomocą stron internetowych, takich jak na przykład **getnada.com**. Dzięki takiemu rozwiązaniu nie będziemy zaśmiecać naszej głównej skrzynki e-mail.

1 Wchodzimy na stronę **getnada.com** **B**. Od razu otworzy się okno z naszą nową skrzynką, jej adres będzie losowy. Skrzynka odświeżana jest automatycznie, więc będziemy mieli dostęp do przychodzących wiadomości. Jest ona aktywna tak długo, dopóki jest otwarta na karcie przeglądarki.

2 Po zamknięciu karty zostanie skasowana po siedmiu dniach. W zupełności wystarczy to do zarejestrowania konta i pobrania konkretnej treści – po chwili możemy zapomnieć o tego typu koncie bez żadnych konsekwencji.

B

YOUR INBOXES
ADD INBOXE +
YOUR INBOXES
cusoheheq@abyssmail.com
NADA TEMP MAIL
CHROME ADDON
Disposable Temporary Email
Your inbox is sacred. Our inboxes are throwaway.
use cusoheheq@abyssmail.com copied!
DELETE THIS INBOX
Subject From Actions
waiting for incoming emails for cusoheheq@abyssmail.com

adam13zajac@gmail.com

Usuwanie treści z internetu

Czasem w internecie dochodzi do wycieku danych. Ktoś może opublikować nasze zdjęcia bez naszej zgody, napisać obraźliwe i nieprawdziwe informacje na nasz temat lub upublicznić jakieś prywatne informacje, które nie powinny znaleźć się w sieci.

Na szczęście możemy starać się usuwać takie treści. Należy jednak pamiętać, aby postępować zgodnie z pewnym ustalonym porządkiem.

Przede wszystkim należy zwrócić się do administratora danej strony z prośbą o usunięcie konkretnej treści, podając swoje argumenty. Możemy dochodzić swoich praw w sądzie, gdyby administrator odmówił usunięcia treści.

Następnie musimy zwrócić się z prośbą do administratorów popularnych wyszukiwarek. Najczęściej prośby o usunięcie z wyników wyszukiwania trafiają do Google, gdyż nawet jeśli administrator usunie obraźliwe informacje na nasz temat, mogą być one nadal wyszukiwane w Google, ponieważ serwis indeksuje i zapisuje witryny na swoich serwerach.

Zgłaszanie usuwania treści z informacjami prywatnymi przez Google

Przeczytajmy, w jaki sposób złożyć prośbę o usunięcie z wyszukiwarki Google prywatnych danych. Według informacji dostępnej na stronie Google, zostanie rozpatrzone usunięcie treści, które zawierają:

- poufne krajowe numery identyfikacyjne – na przykład PESEL
- numer konta bankowego;
- numer karty kredytowej;
- zdjęcie podpisu;
- poufna dokumentacja medyczna.

Wchodzimy na stronę:
https://support.google.com/websearch/troubleshooter/9685456#ts=2889054%2C2889099

Odpowiadamy na kolejne pytania, a następnie wypełniamy formularz. Musimy w nim między innymi podać treści, które chcemy usunąć, i wskazać adresy internetowe, na których znajdują się treści do usunięcia. Dodatkowo warto załączyć zrzuty ekranu, aby osoba, która będzie weryfikować zgłoszenie, mogła szybko odnaleźć treści, o które nam chodzi. Warto również uzasadnić swoje zgłoszenie. By wysłać formularz, klikamy u dołu strony na **Wyślij**.

WYSZUKIWARKA GOOGLE TO NIE WSZYSTKO

Wyszukiwarka Google pokazuje informacje ze stron internetowych. Nawet jeśli usuniemy wskazane treści z wyszukiwarki Google, mogą one wciąż być dostępne w internecie. Oznacza to, że nadal będzie można zobaczyć je na stronie, na której zostały zamieszczone, oraz w mediach społecznościowych, i znaleźć przez inne niż Google wyszukiwarki. Niezbędny może być kontakt z webmasterem witryny i poproszenie go o usunięcie materiałów. Jeśli nie jesteśmy w stanie doprowadzić do usunięcia treści przez właściciela strony, Google może usunąć dane osobowe, w przypadku których istnieje duże ryzyko, że zostaną wykorzystane do kradzieży tożsamości albo dokonania nadużyć finansowych lub innych szkód.

adam13zajac@gmail.com

2 Zachowujemy prywatność w sieci

Zachowanie prywatności podczas korzystania z sieci staje się coraz ważniejsze. Z jednej strony prywatne informacje o nas są łakomym kąskiem dla firm, które handlują danymi w celach reklamowych. Z drugiej polują na nie osoby szukające wycieków danych

Najczęstszą przyczyną, która sprawia, że w ogóle dochodzi do wycieków danych, jest chęć zysku u osób, które takie dane udostępniają.
Publicznie dostępne bazy danych najczęściej zawierają adresy e-mail, hasła, ID kont oraz adresy IP.
Należy dbać o to, aby w razie wycieku naszych danych odpowiednio się zabezpieczyć. Przede wszystkim trzeba jak najszybciej zmienić hasło do konta zarejestrowanego w serwisie, z którego wyciekły dane, i wszystkie podobne dane dostępowe do innych serwisów.

BĄDŹMY BEZPIECZNI W SIECI

Jeśli nie chcemy, aby wyciek naszych prywatnych danych doprowadził do poważnych konsekwencji, starajmy się zawsze stosować do tych zasad:

- Korzystamy z menedżerów haseł i używamy innych haseł do logowania w różnych serwisach
- Jeśli to możliwe, korzystamy wszędzie z autoryzacji dwuskładnikowej
- Korzystamy z VPN, programów AV oraz firewalli
- Zawsze zgłaszamy do odpowiednich służb informację o tym, że staliśmy się ofiarą cyberataku
- Jeśli zamierzamy dokonywać płatności online, wykorzystujemy karty z możliwością doładowania lub wirtualne, na przykład Revolut.
- Unikamy klikania na podejrzane linki – zwłaszcza takie, które nie mają podanej pełnej nazwy, a jedynie skróconą formę.
- Korzystajmy z szyfrowanych aplikacji, na przykład chmury czy komunikatora

Narzędzia dla każdego, które pomogą zachować prywatność

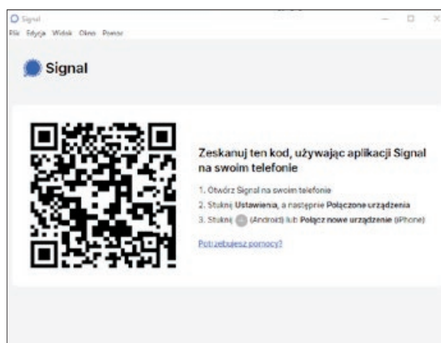
Jeśli poważnie myślimy o zachowaniu prywatności w sieci, należy zacząć stosować odpowiednie programy, które pomogą w osiągnięciu tego celu. Wiele z nich jest polecanych przez takie znane osoby, jak Edward Snowden – specjalista do spraw cyberbezpieczeństwa, który ujawnił program PRISM, czy Elon Musk – biznesmen, dla którego prywatność jest bardzo istotna.

Bezpieczny komunikator

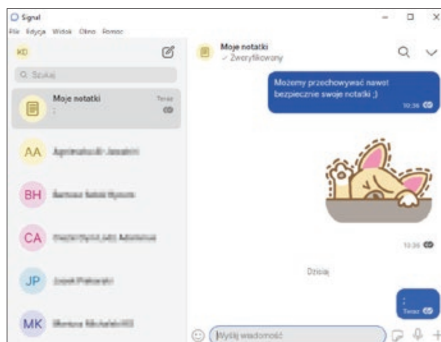
Signal (DVD-KOD: 041) pozwala na wysyłanie wiadomości tekstowych, obrazów, komunikację głosową i wideorozmowy.
Cała komunikacja jest zabezpieczona i nikt nie będzie mógł nas podsłuchać lub sprawdzić, o czym piszemy. Dodatkowo możemy ustawić czyszczenie historii rozmów, dzięki czemu starsze wiadomości same będą znikały.
Signal oferuje również możliwość wprowadzania notatek w jednej z konwersacji – te notatki również są zaszyfrowane.
Zanim zaczniemy korzystać z tego komunikatora w środowisku Windows, wymagana jest jego instalacja na naszym smartfonie. Potrzebny link w postaci kodu QR zostanie wyświetlony bezpośrednio w oknie programu. Po chwili konfiguracji będziemy mogli korzystać z bezpiecznego komunikatora na naszym komputerze.

1 Zanim uruchomimy Signal na komputerze, musimy zainstalować go na naszym smartfonie. Następnie uruchamiamy aplikację na smartfonie i postępujemy zgodnie z instrukcjami na ekranie.

2 W smartfonie naciskamy **Ustawienia**, **Połączone urządzenia**, **+**. Teraz uruchamiamy aplikację Signal na komputerze i skanujemy **kod QR** widoczny na ekranie komputera.



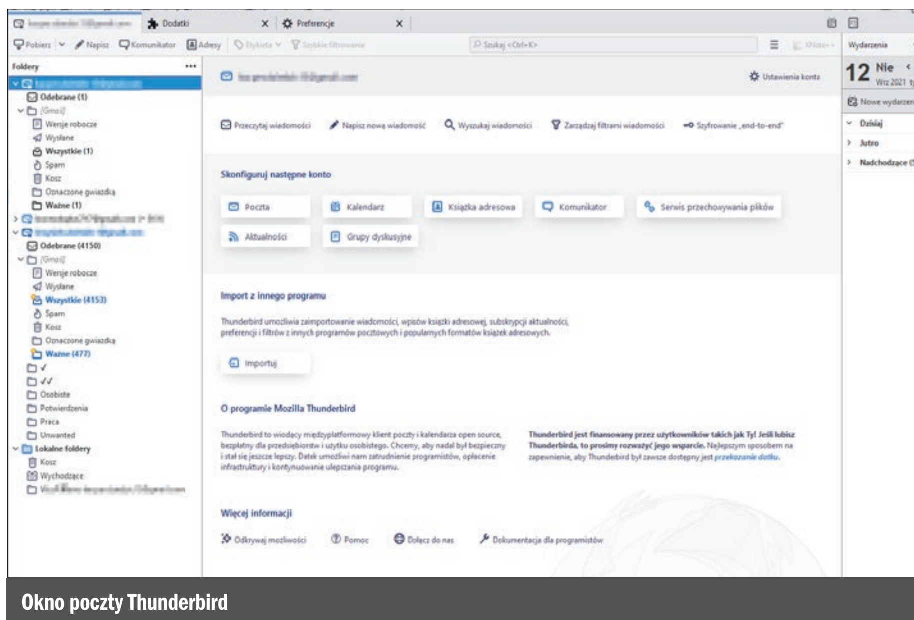
3 Po wykonaniu wszystkich kroków będziemy mogli komunikować się ze znajomymi, wykorzystując komputer do wygodnego wprowadzania wiadomości, a nasze dane będą szyfrowane.



Bezpieczna poczta e-mail

Thunderbird (DVD-KOD: 053/054 32-/64-BIT) to najpopularniejszy bezpłatny program do obsługi poczty e-mail.
Obsługuje wiele skrzynek pocztowych, ma książkę adresową, funkcję filtrowania niechcianej korespondencji (spamu), umożliwia też szybkie przeszukiwanie poczty i importowanie jej z innych programów. Wygląd interfejsu można zmieniać za pomocą motywów graficznych, program obsługuje również do-

adam13zajac@gmail.com



Okno poczty Thunderbird

datki (podobnie jak Firefox), dzięki którym możemy zwiększać jego możliwości i dopasowywać go do własnych potrzeb. Dodatkowym atutem jest filtr antyphishingowy, który pozwoli uniknąć fałszywych ofert.

Ważne! Thunderbird wspiera szyfrowanie wiadomości typu end-to-end, co oznacza, że wiadomość zaszyfrowana po naszej stronie zostanie dopiero odszyfrowana przez naszego odbiorcę i nikt po drodze nie będzie mógł poznać treści takiej wiadomości.
Więcej o obsłudze tego programu i możliwości korzystania z szyfrowania przeczytamy od strony 51.

Przechowujemy hasła

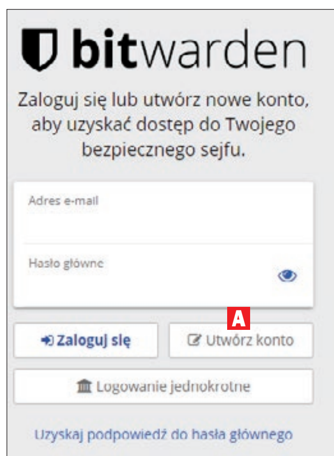
Bitwarden (**DVD-KOD: 004/005** PORTABLE) to nowoczesny menedżer haseł i sejf na poufne informacje, rozwijany jako projekt open source.
W programie można bezpiecznie przechowywać dane logowania do wielu stron, dane kart płatniczych, informacje o naszej tożsamości, poufne notatki oraz inne rodzaje wrażliwych informacji. Dane przechowywane w Bitwardenie szyfrowane są silnym algorytmem AES-256 typu end-to-end i można je synchronizować pomiędzy naszymi komputerami (Windows, macOS, Linux), telefonami i tabletami (Android, iOS) poprzez darmowe konto Bitwarden.
Program można także zintegrować z najpopularniejszymi przeglądarkami WWW za pomocą rozszerzeń.
Zanim zaczniemy używać naszego bezpiecznego programu, musimy utworzyć konto, z którego będziemy mogli korzystać na wielu urządzeniach.

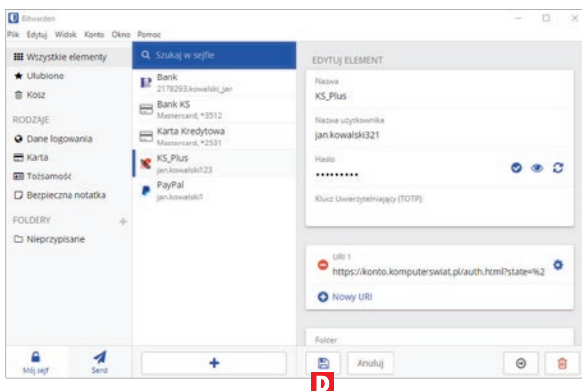
1 Po uruchomieniu programu klikamy na **Utwórz konto** **A**.

2 Wypełniamy formularz niezbędnymi danymi i klikamy na **Wyślij**.

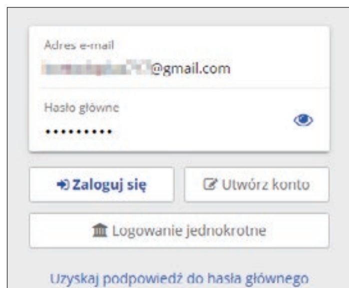
Uwaga! Upewnijmy się, że hasło do naszego konta będzie bardzo złożone, gdyż jeśli ktoś je odgadnie, uzyska dostęp do wszystkich naszych haseł.

adam13zajac@gmail.com





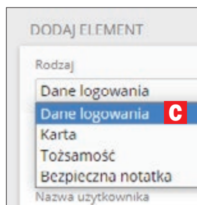
3 Następnie od razu możemy się zalogować do naszego konta – nie musimy potwierdzać żadnych wiadomości e-mail. Podajemy dane i klikamy na **Zaloguj się**.



4 Możemy teraz dodawać wpisy zawierające informacje o konkretnych stronach, kartach i hasłach. Klikamy na symbol **+** **B** u dołu okna programu. Następnie po prawej stronie w polu **Rodzaj** wybieramy element, jaki chcemy dodać, na przykład numer karty lub dane logowania **C**.

5 Po podaniu niezbędnych danych klikamy na ikonę dyskietki u dołu okna **D**.





6 Dodawane elementy na bieżąco są szyfrowane i synchronizowane z chmurą w internecie, dzięki temu po chwili te same dane będziemy mogli odczytać na przykład na smartfonie.

Szyfrowane łącze z internetem

Windscribe VPN (**DVD-KOD: 061**) to markowy VPN, który w podstawowej, darmowej wersji oferuje bezpłatny pakiet danych 10 GB miesięcznie.

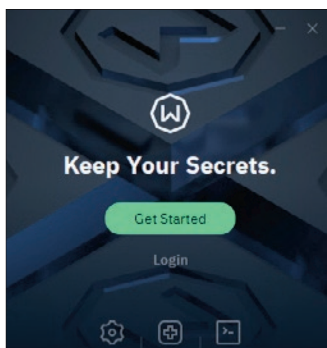
Program ma prosty, nowoczesny interfejs i oprócz wersji instalowanej w Windows może działać jako rozszerzenie do przeglądarki Chrome, Firefox, Opera, Edge, jako aplikacja mobilna na smartfon lub tablet (Android, iOS). Ma też wersje na macOS i Linuxa. Oferuje silne szyfrowanie połączenia z internetem, aby przesyłane przez nas informacje nie mogły być odczytane przez dostawcę usług internetowych ani operatora sieci Wi-Fi.

Chroni również naszą prywatność – oprócz ukrywania naszego adresu IP, co pozwala omijać różnego typu internetowe blokady i anonimowo publikować w sieci, ma również funkcje do blokowania trackerów, malware'u i reklam. Do konta użytkownika nie ma przypisanego limitu urządzeń.

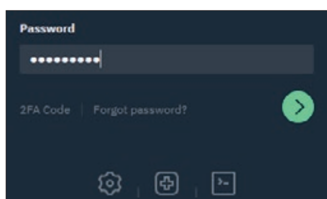
Korzystamy z VPN

1 Instalujemy Windscribe VPN, uruchamiamy go, zakładamy konto i klikamy na link potwierdzający w wiadomości e-mail.

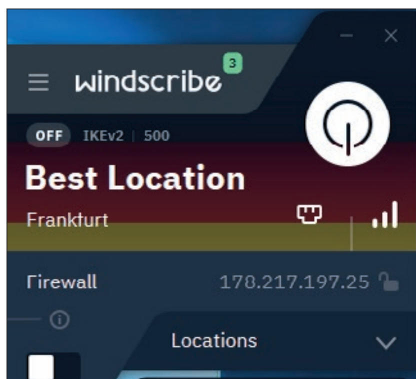
adam13zajac@gmail.com



2 Następnie możemy zalogować się do programu – po podaniu danych klikamy na zieloną strzałkę w celu zalogowania.

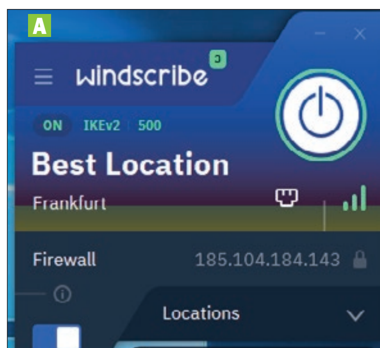


3 Teraz wystarczy kliknąć na symbol zasilania w celu aktywowania połączenia VPN z wybranym serwerem.



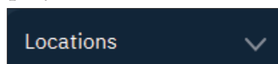
4 Po nawiązaniu bezpiecznego połączenia wygląd okna aplikacji zostanie zmieniony na niebieski **A**.

5 W celu przerwania połączenia VPN ponownie klikamy na symbol **ON/OFF**.

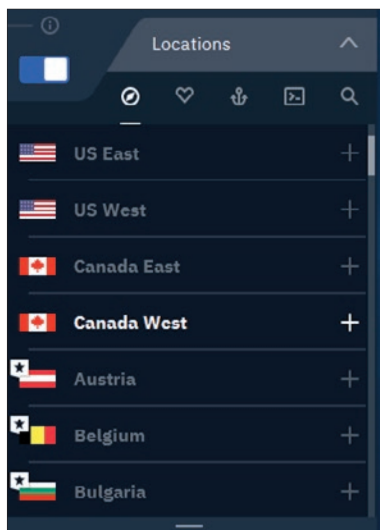


Zmieniamy serwer

Jeśli chcemy zmienić serwer, z którym łączymy się automatycznie, należy kliknąć na strzałkę przy nazwie serwera.



Następnie z listy wybieramy serwer, z którym chcemy się połączyć – serwery oznaczone gwiazdką są przeznaczone dla użytkowników wersji płatnej.

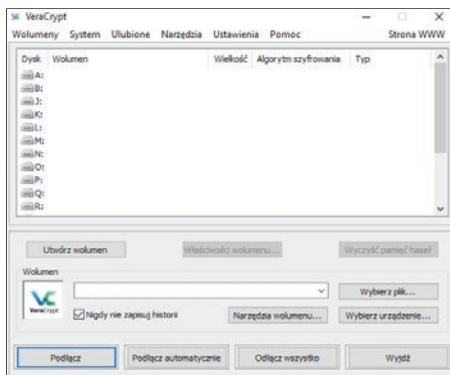


Narzędzie do szyfrowania danych

Jeśli interesuje nas maksymalne bezpieczeństwo naszych nośników danych, warto skorzystać z pomocy programu **VeraCrypt**

adam13zajac@gmail.com

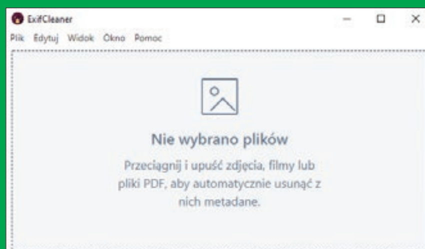
(DVD-KOD: 057/058 PORTABLE). Możemy zaszyfrować cały dysk, wybrane partycje, a nawet wybrane nośniki USB. Często przenosimy poufne dane na pendrive'ach, a są one najbardziej podatne na kradzież lub zgubienie. Jeśli będą odpowiednio przez nas zabezpieczone, osoby trzecie nie uzyskają dostępu do naszych danych. Opis krok po kroku procesu szyfrowania danych znajdziemy w rozdziale **4** od strony 34, dowiemy się tam, jak zaszyfrować cały system oraz jak utworzyć przenośny sejf na dane na nośniku USB.



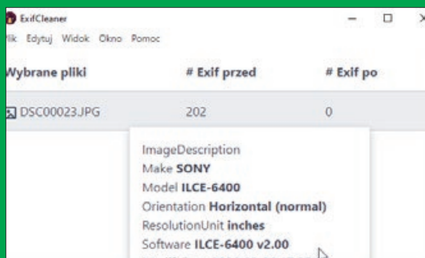
CZYŚCIMY METADANE Z PLIKÓW MULTIMEDIALNYCH – EXIFCLEANER

ExifCleaner (DVD-KOD: 012) to darmowe narzędzie open source do usuwania metadanych EXIF ze zdjęć i filmów metodą przeciągnij i upuść. Program obsługuje najpopularniejsze formaty graficzne (JPG, PNG, TIF, GIF), wideo (MP4, M4A, MOV, QT), a także usuwanie metadanych z dokumentów PDF. Obsługuje ciemny tryb interfejsu, ma też funkcję wielordzeniowego przetwarzania wsadowego, która pozwala szybko przetwarzać wiele plików naraz. ExifCleaner jest zbudowany na bazie sprawdzonej biblioteki ExifTool i wieloplatformowego frameworka Electron. Oprócz wersji na Windows jest dostępny na systemy macOS i Linux. Usuwając takie dane przed wrzuceniem zdjęcia do internetu, chronimy własną prywatność, gdyż do zdjęcia może być przypisanych wiele znaczników, które mogą zdradzać naszą lokalizację czy urządzenie, z którego wykonaliśmy zdjęcie.

1 W celu usunięcia metadanych z pliku multimedialnego po uruchomieniu programu ExifCleaner przeciągamy do jego okna wybrane pliki.



2 Po załadowaniu pliku będziemy mogli zapoznać się z wszystkimi danymi, jakie przypisane są do naszego pliku. W naszym przykładzie są to 202 unikalne informacje, w tym model kamery i wiele innych. Dane po wczytaniu pliku zostaną automatycznie usunięte. Nie musimy nic konfigurować. **Uwaga! Operacja jest nieodwracalna.**



Na kolejnych stronach poznamy jeszcze wiele innych programów, które pozwalają na zachowanie prywatności i anonimowości, w tym system Whonix i przeglądarkę Tor Browser.

Co wiemy o programach do szpiegowania

Wielu użytkowników internetu nie zdaje sobie sprawy z tego, że od wielu lat trwa wręcz otwarta wojna pomiędzy twórcami oprogramowania do szpiegowania a deweloperami, którzy starają się stworzyć programy dające użytkownikom jak największą prywatność, blokując możliwości podsłuchu. Najczęściej w najbardziej złożone programy są zaangażowane rządy rozwiniętych państw.

Jednym z pierwszych narzędzi, o których zrobiło się naprawdę głośno, był **PRISM**, tajny amerykański program szpiegowski. PRISM jest aktywny od 2007 roku i umożliwia NSA dostęp do serwerów największych przedsiębiorstw internetowych, jak również gromadzenie ich danych na własny użytek. Oznacza to, że inwigilacji podlegają wszyscy, którzy korzystają z usług takich firm, jak Google, Microsoft, Facebook czy Apple. Z ujawnionych dokumentów wynika, że firmy te zgodziły się na działanie tego programu.

Udostępniane NSA dane to między innymi wiadomości pocztowe, zasoby dysków internetowych, zdjęcia i filmy, dane przekazywane jako transfer plików, dane z komunikatorów tekstowych i wideo, dane z serwisów społecznościowych, jak również loginy.

Informacje o tym zostały ujawnione przez Edwarda Snowdena i potwierdzone przez dyrektora centrali wywiadu.





Zagrożenie prywatności jest ogromne, gdyż program PRISM obejmuje oficjalnie dane przepływające przez serwery w USA, co oznacza, że mogą być inwigilowani użytkownicy z całego świata.

Na świecie jest więcej tego typu programów. USA do inwigilacji korzysta też na przykład z programu **XKeyscore**. Dane z 2013 roku wskazują na to, że NSA korzysta z tego systemu, który jest w stanie zbierać dane z całego internetu, z każdej skrzynki pocztowej i każdej witryny. W systemie można oznaczać użytkowników specjalnymi flagami i śledzić bez przerwy ich poczynania w sieci. Po utworzeniu profilu online możemy być bez przerwy inwigilowani. Co ciekawe, w 2014 roku ujawniono, że automatycznie oznaczano w tym programie osoby, które korzystały z sieci Tor, poszukiwały oprogramowania chroniącego prywatność i interesowały się dystrybucją systemu Linux Tails.

W Polsce głośno zrobiło się o programie **Pegasus**, ale wiele państw korzysta z tego programu. Jest to nieco mniej rozbudowane narzędzie, które służy do infekowania urządzeń z systemem iOS i częściowo Android. W przypadku urządzeń firmy Apple możliwe było zainfekowanie urządzenia zupełnie zdalnie. A w przypadku urządzeń z Androidem konieczna była interakcja użytkownika lub osób trzecich.

Można wykryć i rozpoznać działanie Pegasusa. Jak sprawdzić, czy nasz smartfon jest zainfekowany i jak go chronić, dowiemy się z rozdziałów **7** i **8**.

adam13zajac@gmail.com

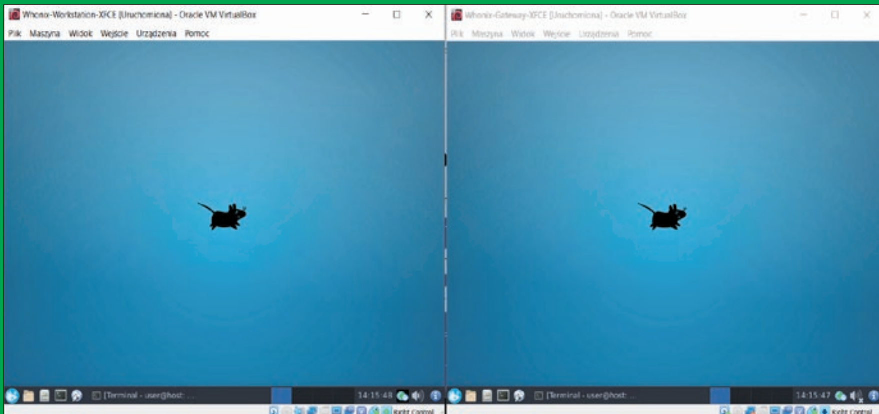
JAK SIĘ BRONIĆ PRZED SZPIEGOWANIEM

Jeśli naprawdę chcemy całkowicie ochronić się przed szpiegowaniem, powinniśmy korzystać z systemów operacyjnych, które umożliwiają pozostanie całkowicie anonimowym. Jednym z nich jest **Tails**. Cały ruch sieciowy przepuszcza on przez serwery sieci Tor, która do tej pory według audytów nadal nie pozwala na śledzenie w sieci – oczywiście o ile będziemy korzystać z niej z rozwagą.



Tails – system dla fanów anonimowości, pozwala stać się naprawdę anonimowym w sieci, jednak musimy go uruchamiać jako osobny system, na przykład z dysku przenośnego, i nie możemy w tym samym czasie korzystać z naszego głównego systemu

Drugą ciekawą opcją jest system **Whonix** (DVD-KOD: 060) – przeczytamy, jak z niego korzystać, w rozdziale **6**. Ten system jeszcze bardziej stawia na anonimowość, ochronę prywatności i bezpieczeństwo użytkownika. Wymusza aktualizację programowania przed uruchomieniem systemu. Cały ruch kieruje przez sieć Tor. Składa się z dwóch wirtualnych maszyn. Najpierw uruchamiana jest „brama", a później „stacja robocza". Pozwala to na ochronę przed wyrafinowanymi atakami. Do tej pory system ten przeszedł wszystkie audyty bezpieczeństwa.



Whonix – system, który uruchamiamy przy wykorzystaniu dwóch wirtualnych maszyn. Możemy z niego korzystać wewnątrz Windows, MacOS oraz Linuxa. Skutecznie chroni naszą prywatność i umożliwia normalną pracę w domyślnym dla nas systemie

Korzystając z bezpiecznego oprogramowania i systemów oraz sieci anonimizujących jesteśmy w stanie ukryć się przed programami szpiegującymi.

Zbieranie prywatnych informacji przez Windows – jak odzyskać kontrolę

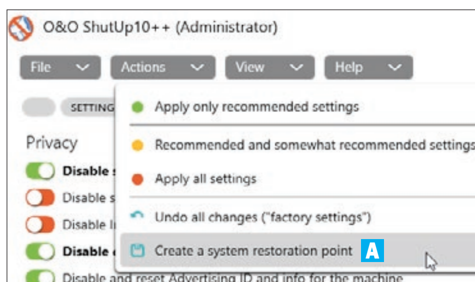
Ze zbierania informacji o użytkownikach szczególnie znany jest Windows 10, wciąż najbardziej popularna wersja systemu Microsoftu – wywołało to sporo krytyki po premierze Dziesiątki.
Obecnie zarówno system Windows 10, jak i najnowszy Windows 11 nadal zbierają dane o użytkownikach, jednak teraz użytkownicy są pytani o wiele ustawień przed pierwszym uruchomieniem systemu. Dodatkowo znacznie mniej danych jest wysyłanych bez wiedzy użytkowników.
Jeśli jednak chcemy mieć nad tym kontrolę, warto skorzystać z programu **O&O ShutUp10** (**DVD-KOD: 026**). Działa on zarówno w systemie Windows 10, jak i w Windows 11. Służy do wyłączania funkcji szpiegujących i kontroli ustawień prywatności. Aplikacja ta pozwala zapanować nad danymi wysyłanymi do Microsoftu, jednocześnie chroniąc nas przed potencjalnymi lukami w zabezpieczeniach systemu.

Tworzymy punkt przywracania systemu

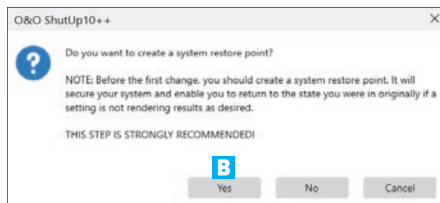
Zanim zaczniemy wprowadzać zmiany za pomocą O&O ShutUp10, powinniśmy na wszelki wypadek stworzyć punkt przywracania systemu. Dzięki temu nawet jeśli po wprowadzonych przez nas zmianach Windows zacznie szwankować, będziemy mogli przywrócić go do poprawnej pracy.

1 Po uruchomieniu programu **O&O ShutUp10** klikamy na górnym pasku na **Actions**, **Create system restoration point** **A**.

2 Następnie musimy kliknąć na **Yes** **B**, by potwierdzić polecenie wykonania punktu przywracania systemu.



3 Po chwili punkt zostanie utworzony, a my możemy zacząć wprowadzać zmiany bez obaw o stabilną pracę systemu.



Wybieramy bezpieczne ustawienia

Po prawej stronie okna O&O ShutUp10 znajduje się kolumna **Recommended** **C**. Znajdziemy w niej trzy domyślne profile: **Zielony**, **Żółty** i **Czerwony**.
Zalecany jest wybór tego pierwszego, ponieważ jest on najmniej ryzykowny i obejmuje większość istotnych zmian w systemie, które uniemożliwiają śledzenie.

1 Na górnym pasku klikamy na **Actions**, **Apply only recommended settings** **D**.

2 Po wprowadzeniu zmian konieczne będzie ponowne uruchomienie systemu w celu ich wprowadzenia.

adam13zajac@gmail.com

O&O ShutUp10++ (Administrator)

File | Actions | View | Help | Search

Apply only recommended settings **D**

Recommended and somewhat recommended settings

Apply all settings

Undo all changes ("factory settings")

Create a system restoration point

SETTING | RECOMMENDED **C**

Privacy

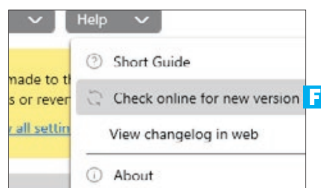
Disable	yes
Disable s	yes
Disable l	yes
Disable	yes
Disable and reset Advertising ID and info for the machine	yes
Disable and reset Advertising ID and info for current user	yes
Disable transmission of typing information	yes
Disable advertisements via Bluetooth	yes
Disable the Windows Customer Experience Improvement Program	yes
Disable backup of text messages into the cloud	yes
Disable suggestions in the timeline	yes
Disable suggestions in Start	yes
Disable tips, tricks, and suggestions when using Windows	yes
Disable showing suggested content in the Settings app	yes

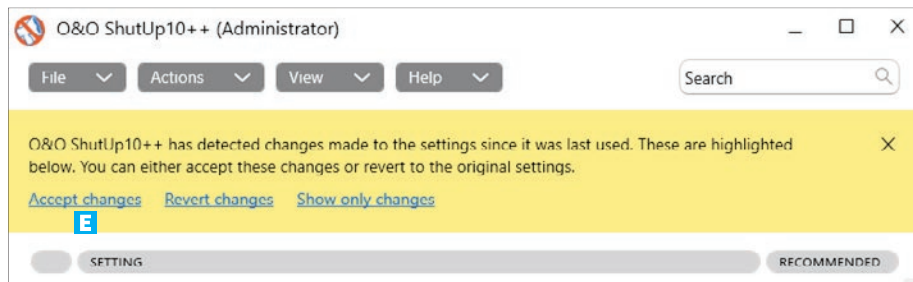
Find new versions at: https://www.oo-software.com/ — O&O software

3 Po ponownym uruchomieniu komputera, a także potem, po dokonaniu zmian przez inne programy, za każdym razem, gdy włączymy O&O ShutUp10, otrzymamy informację, że ustawienia systemu różnią się od tych, przy których ostatni raz konfigurowaliśmy program. Zmiany zostaną wskazane przez pogrubienie opisów opcji.

4 Możemy od razu zaakceptować wszystkie zmiany, klikając na **Accept changes** **E**.

5 Warto co jakiś czas przeprowadzać aktualizację aplikacji. W tym celu należy na górnym pasku kliknąć na **Help**, a potem na **Check online for new version** **F**.





adam13zajac@gmail.com

3 Usuwamy ślady z naszego komputera

Wystarczy, że ktoś na chwilę uzyska dostęp do naszego laptopa, a będzie mógł szybko zdobyć wiele danych. W tym rozdziale przeczytamy, jak zadbać o to, by w komputerze nie zostawiać śladów, na podstawie których niepowołana osoba może zbyt wiele się o nas dowiedzieć

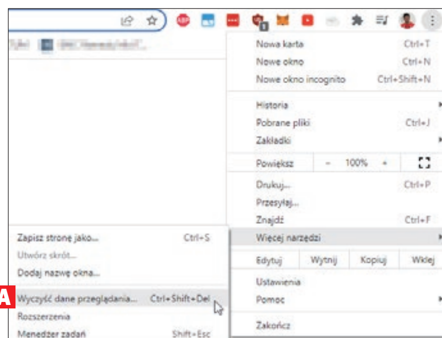
Usuwamy dane z przeglądarek

Większość użytkowników przeglądarek internetowych nawet nie zdaje sobie sprawy, jak wiele informacji na ich temat jest gromadzonych zarówno na samym komputerze, jak i w serwisach, do których się logują. Jest to z pewnością bardzo wygodne, gdy możemy na smartfonie szybko uzyskać dostęp do witryn odwiedzonych wcześniej na komputerze czy też automatycznie logować się do wielu serwisów. Jednak zwiększa to również ryzyko uzyskania przez osoby trzecie dostępu do naszych kont i profili. Wystarczy, że ktoś usiądzie przy naszym laptopie lub pececie na chwilę i już może poznać nasze hasła do wielu usług.
Dlatego, jeśli z naszego komputera może skorzystać ktoś poza nami, bardzo istotne jest dbanie o to, żeby nasze hasła nie były zapisywane przez przeglądarkę i by wyniki naszych wyszukiwań były usuwane.
Zobaczmy na przykładzie kilku popularnych przeglądarek, jak pozbyć się historii i innych śladów, jakie zostawiamy, oraz plików cookie.

Warto także zabezpieczyć komputer w taki sposób, aby nikt nie mógł uzyskać do niego dostępu bez hasła.

Google Chrome

W Chrome możemy skasować wszystkie ślady w jednym menu, co jest bardzo wygodne. Dodatkowo warto pamiętać, że jeśli nie chcemy, żeby przeglądarka zapisywała dane z jakiejś sesji, powinniśmy uruchomić tryb



adam13zajac@gmail.com

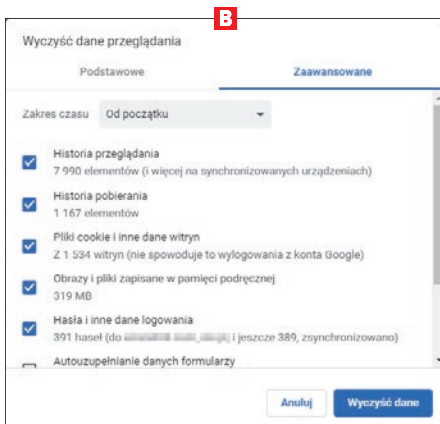
incognito. (Więcej o trybie incognito przeczytamy w dalszej części rozdziału).

1 W celu usunięcia historii z Google Chrome po uruchomieniu przeglądarki klikamy w górnym prawym rogu na trzy kropki.

2 Przechodzimy do **Więcej narzędzi** i klikamy na **Wyczyść dane przeglądania** **A**.

3 Pojawi się okno **B**, w którym będziemy mogli skonfigurować opcje czyszczenia danych przeglądarki.

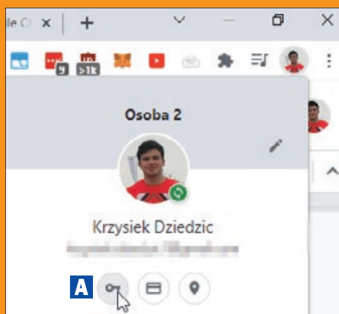
4 W zakładce **Podstawowe** nie będziemy w stanie usunąć wszystkich danych przeglądania. Należy przejść do zakładki **Zaawansowane**. Możemy na niej wybrać wszystkie dane, w tym zapisane hasła, historię pobierania i danych formularzy. Jeśli chcemy usunąć wszystkie dane, należy wybrać **Zakres cza-**



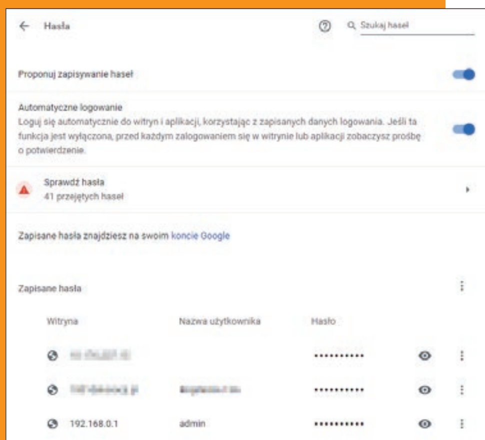
UZYSKUJEMY DOSTĘP DO WSZYSTKICH ZAPISANYCH HASEŁ W GOOGLE CHROME

Jeśli sami będziemy potrzebowali sprawdzić hasło do konkretnego serwisu, możemy to szybko zrobić w zapisanej bazie w przeglądarce.

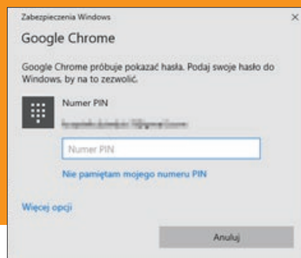
1 Po uruchomieniu przeglądarki Google Chrome klikamy w prawym górnym rogu na nasz awatar, a następnie na ikonę **Hasła** **A**.



2 Uzyskamy w ten sposób dostęp do karty z zapisanymi w przeglądarce hasłami. W celu wyświetlenia konkretnego hasła należy kliknąć na symbol oka.



3 Zanim hasło zostanie wyświetlone, pojawi się prośba o podanie hasła do systemu Windows.



su: Od początku. Po wybraniu opcji klikamy na **Wyczyść dane.**

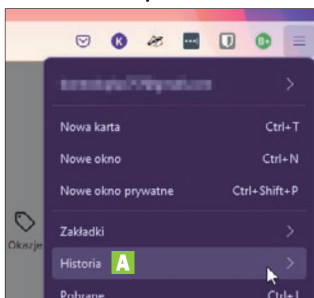
5 W przeglądarce z przykładu zapisanych jest aż 391 haseł. Można sobie wyobrazić, co by się mogło stać, gdyby te dane trafiły w niepowołane ręce.

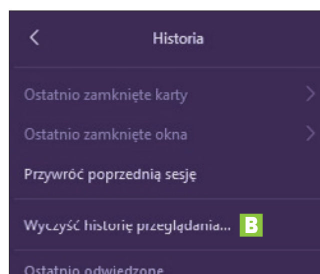
Mozilla Firefox

W przeglądarce Firefox również możemy wyczyścić wszystkie dane, korzystając z jednego menu.

1 Po uruchomieniu przeglądarki klikamy w górnym prawym rogu okna na trzy kreski, a potem na **Historia** A.

2 Następnie klikamy na **Wyczyść historię przeglądania** B.



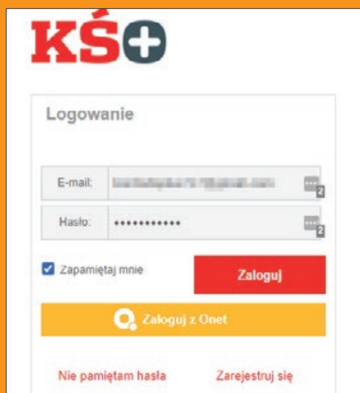


POZNAJEMY HASŁA BEZ KONIECZNOŚCI PODANIA HASŁA ADMINISTRATORA

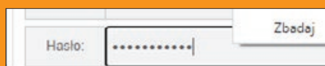
Istnieją sposoby na poznanie hasła zapisanego w przeglądarce bez konieczności podawania jakichkolwiek danych autoryzacyjnych. Musimy jedynie aktywować autouzupełnianie haseł.

1 Przechodzimy do witryny, dla której mamy w przeglądarce zapisane hasło.

2 Dane logowania powinny pojawić się w odpowiednich polach.



3 Klikamy na pole z hasłem prawym przyciskiem myszy i wybieramy opcję **Zbadaj**.

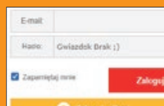


4 Zostanie otworzone narzędzie dewelopera z podświetlanym elementem w kodzie strony, który nas interesuje.

```
▾<li class>
  <label class="inputData" for="f_password">Hasło:</label>
  <input type="password" id="f_password" name="password" class="correct" style=
  "background-image: url("data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAA
  BCAQAAAC1HAwCAAAAC0lEQVR4nGP6zwAAAgcBApocMXEAAAAASUVORK5CYII="); cursor: aut
  o;" autocomplete="off"> == $0
  </li>
```

5 Klikamy na **type="password"** i zmieniamy wartość parametru na **text**, po czym akceptujemy zmiany, wciskając klawisz enter.

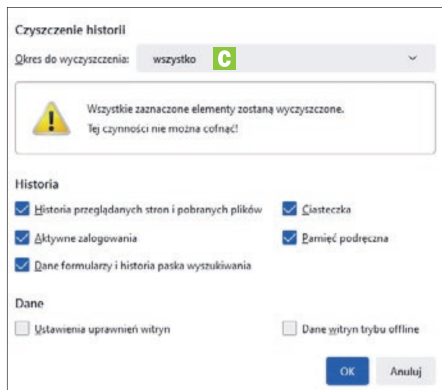
```
<label class="inputData" f
<input type="text" id="f p
kground-image: url("data:i
AAAC1HAwCAAAAC0lEQVR4nGP6z
```



6 Teraz pole z hasłem nie będzie maskowane gwiazdkami i będziemy mogli poznać hasło, jakie się pod nimi kryło.

adam13zajac@gmail.com

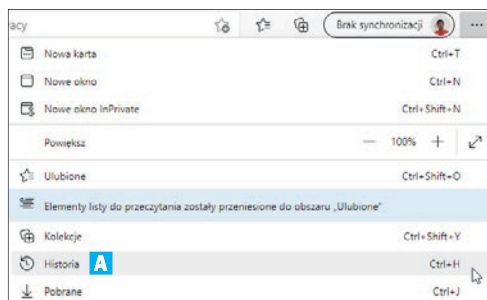
3 Wybieramy **Okres do wyczyszczenia: wszystko** **C**, zaznaczamy elementy do usunięcia i klikamy na **OK**.



Microsoft Edge

W najnowszej przeglądarce Microsoftu również możemy skasować wszystkie dane, korzystając z jednego menu. Dodatkowo możemy też zaznaczyć opcję, która pozwoli na automatyczne kasowanie wszystkich danych przy zamykaniu przeglądarki, co może okazać się bardzo przydatne.

1 Po uruchomieniu przeglądarki klikamy w prawym górnym rogu na trzy kropki, a następnie na **Historia** **A**.

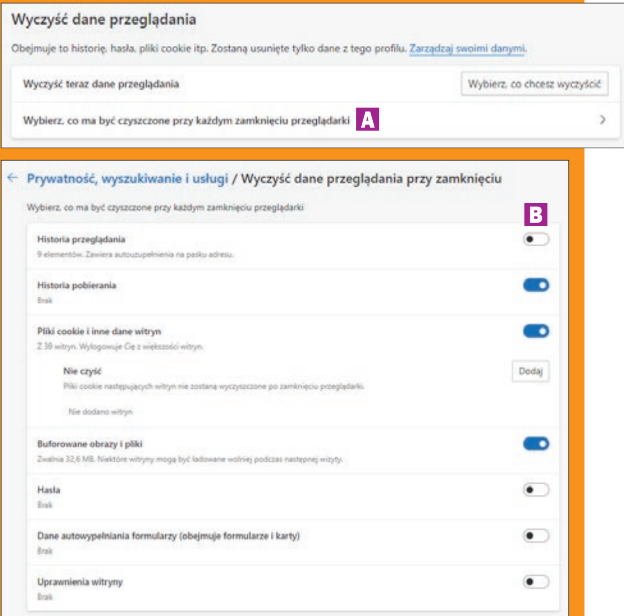


AUTOMATYCZNE CZYSZCZENIE PRZY ZAMYKANIU PRZEGLĄDARKI – EDGE

W ustawieniach przeglądarki w sekcji **Prywatność, wyszukiwanie i usługi** w polu **Wyczyść dane przeglądania** możemy skonfigurować opcję automatycznego czyszczenia danych przy zamykaniu przeglądarki.

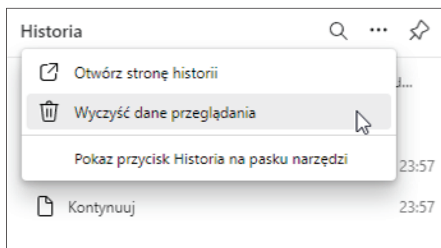
1 Klikamy na **Wybierz, co ma być czyszczone przy każdym zamknięciu przeglądarki** **A**.

2 W kolejnym oknie będziemy mogli skonfigurować, które elementy mają być czyszczone każdorazowo przy zamykaniu przeglądarki. Wystarczy klikać na wybrane przełączniki **B**.

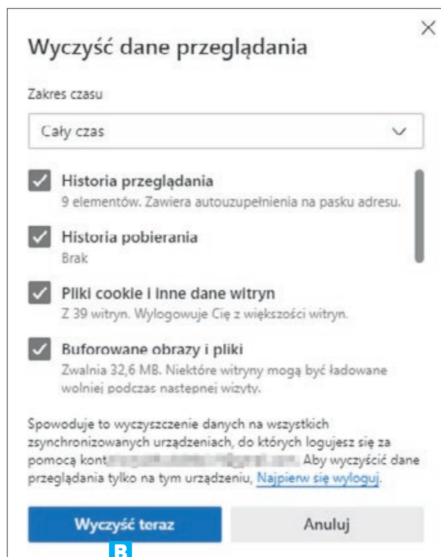


adam13zajac@gmail.com

2 Teraz ponownie klikamy na trzy kropki i wybieramy z menu opcję **Wyczyść dane przeglądania**.

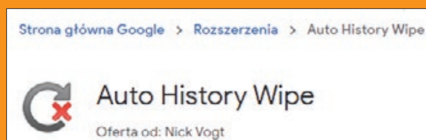


3 Następnie wskazujemy, jakiego typu dane chcemy usunąć, wybieramy odpowiedni zakres czasu i klikamy na **Wyczyść teraz** **B**.

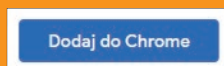


AUTOMATYCZNE USUWANIE DANYCH PRZEGLĄDANIA W CHROME

Jeśli zależy nam tylko i wyłącznie na czyszczeniu danych przeglądania w przeglądarce Google Chrome, możemy zainstalować odpowiedni dodatek, na przykład Auto History Wipe – **https://chrome.google.com/webstore/detail/auto-history-wipe**



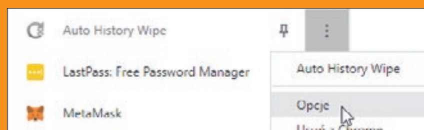
1 Instalujemy dodatek, klikając na **Dodaj do Chrome**.



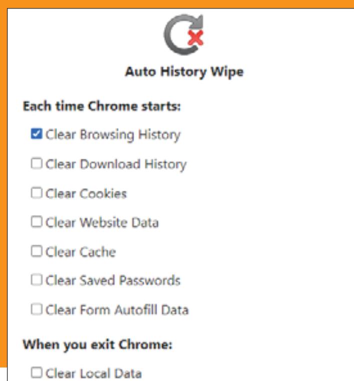
2 Potwierdzamy dodanie, klikając na **Dodaj rozszerzenie**.



3 Następnie na pasku z rozszerzeniami klikamy na dodatek prawym przyciskiem myszy i wybieramy **Opcje**.



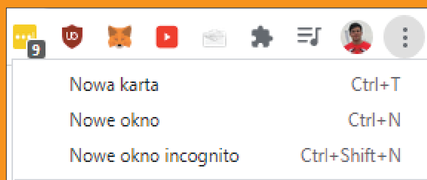
4 W tym widoku możemy skonfigurować, jak ma działać zainstalowany dodatek, a konkretniej, jakie dane mają być czyszczone.



KORZYSTAMY Z TRYBU PRYWATNEGO – INCOGNITO

Wszystkie popularne przeglądarki oferują specjalny tryb, który pozwala po zamknięciu sesji przeglądania wyczyścić wszelkie zapisane dane.
W Chrome taki tryb nazwany jest **incognito**, w Firefoxie – **Okno prywatne**, a w Edge – **InPrivate**.

1 Jeśli chcemy korzystać z tego trybu, po uruchomieniu przeglądarki wystarczy kliknąć na ikonę menu podręcznego i wybrać z niego tryb prywatnego przeglądania, czyli na przykład w Chrome – **Nowe okno incognito**.



2 W takiej sesji możemy normalnie korzystać z przeglądarki, ale po jej zamknięciu dane przeglądania zostaną wykasowane automatycznie. Pamiętajmy jednak, że tryb prywatny nie zapewnia nam żadnej anonimowości w internecie, a jedynie pozwala wygodnie zatrzeć ślady przeglądania na samym urządzeniu.

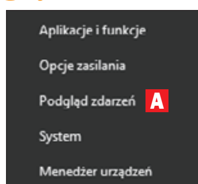


Dziennik systemu Windows – co w nim można znaleźć i jak go wyczyścić?

Zacznijmy od tego, czym jest dziennik zdarzeń w systemie Windows, czyli funkcja o nazwie **Podgląd zdarzeń**. Otóż jest to składnik systemu, który odpowiada za przechowywanie wszelkiego typu informacji dotyczących aktywności komputera. Wpisy, które są w nim tworzone, odnoszą się do uruchamianych usług, włączania ważnych aplikacji, a nawet wciskania fizycznego przycisku zasilania. Jest to bardzo przydatne narzędzie, które może pomóc nam zdiagnozować problemy występujące w naszym systemie czy w komputerze. Może jednak także stać się źródłem wiedzy na nasz temat – w dzienniku zapisywane są dokładne czasy wszystkich ważnych akcji. Dzięki temu ktoś, kto uzyska dostęp do Podglądu zdarzeń, będzie w stanie określić dokładnie, w jakich godzinach korzystaliśmy z komputera, kiedy go uruchomiliśmy i wyłączyliśmy. Z punktu widzenia zachowania prywatności warto co jakiś czas czyścić wpisy dziennika systemowego, zwłaszcza jeśli nie występują żadne problemy techniczne w naszym urządzeniu.

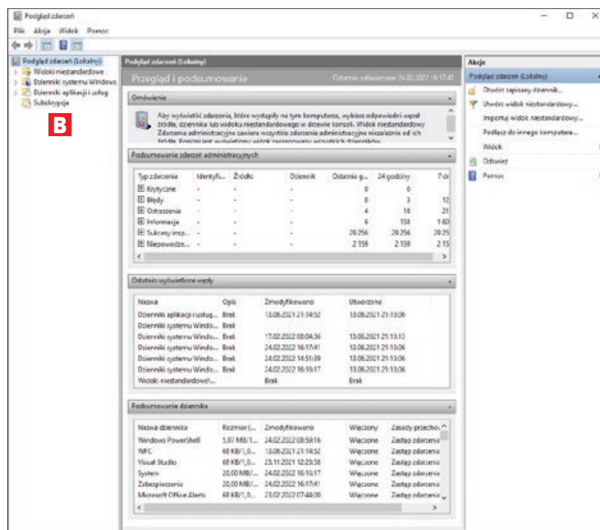
Jak uruchomić podgląd zdarzeń?

1 Klikamy prawym przyciskiem myszy na menu **Start**, a następnie z listy wybieramy opcję **Podgląd zdarzeń** **A**.



adam13zajac@gmail.com

2 Teraz po lewej stronie zauważymy drzewo katalogów. Wszystkie zapisywane zdarzenia są umieszczane w odpowiednich katalogach **B**, dzięki czemu łatwiej dotrzeć do tego, czego szukamy.



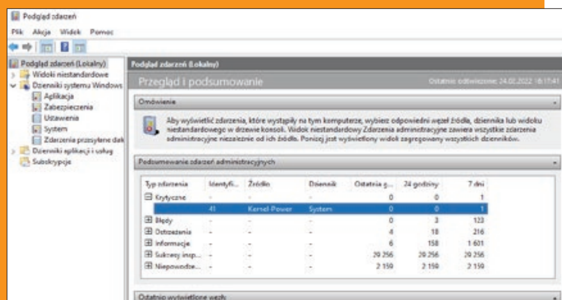
Korzystamy z podglądu zdarzeń i dzienników

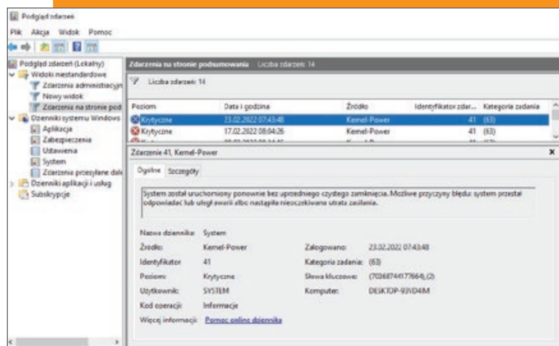
Ta funkcja systemu Windows przydaje się głównie do diagnostyki, ponieważ odnotowuje błędy występujące w systemie oraz, jak już wiemy, pozwala sprawdzić, kto, w jakich godzinach i w jaki sposób korzystał z komputera.

SZYBKA DIAGNOSTYKA

Jeśli chcemy szybko sprawdzić najważniejsze błędy, możemy skorzystać z widoku podsumowania dostępnego od razu po uruchomieniu **Podglądu zdarzeń**.

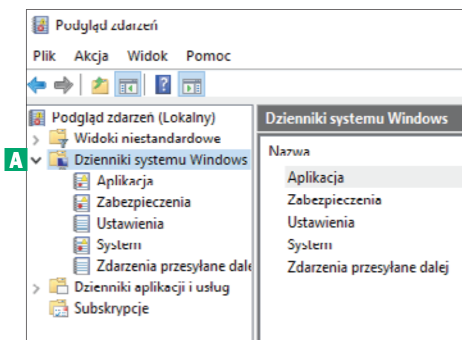
1 W środkowej części ekranu rozwijamy kategorię zdarzeń, która nas interesuje, a potem dwukrotnie klikamy na zdarzenie, któremu chcemy się bliżej przyjrzeć.





2 W naszym przykładzie jest to jedno z najczęstszych zdarzeń krytycznych – zdarzenie z identyfikatorem **41** informujące o tym, że komputer został uruchomiony ponownie bez wcześniejszego poprawnego zamknięcia. Jeśli wrócimy do komputera, który samoczynnie się ponownie uruchomi, możemy w ten sposób sprawdzić, czy przez chwilę nie było prądu, czy powód ponownego uruchomienia był inny.

adam13zajac@gmail.com



1 Po uruchomieniu Podglądu zdarzeń po lewej stronie klikamy na strzałkę przy kategorii **Dzienniki systemu Windows** **A**, w celu jej rozwinięcia.

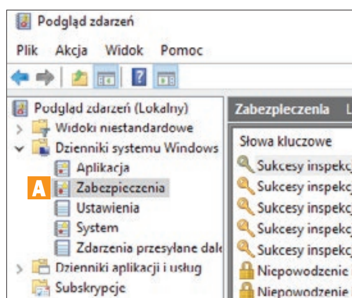
2 Teraz przechodzimy do wybranej zakładki, na przykład **System**, i klikamy na **Poziom** w celu posortowania informacji i łatwiejszego znalezienia błędów.

3 Po znalezieniu błędu **B** i kliknięciu na niego na dole ekranu pojawią się szczegółowe informacje modułu lub aplikacji, która sprawia problem. Dzięki temu możemy szukać dalszej pomocy w sieci, podając również identyfikator błędu i jego źródło.

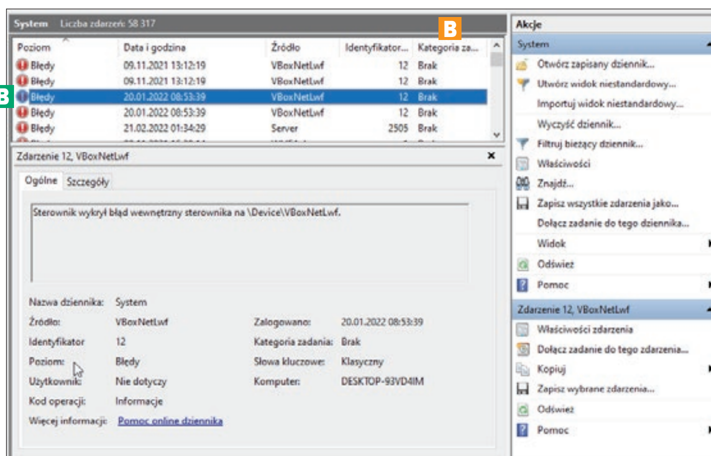
Sprawdzamy czas trwania zalogowanej sesji

Podgląd zdarzeń w systemie Windows pozwala z bardzo dużą dokładnością stwierdzić, jak długo dany użytkownik był zalogowany. Po pierwsze daje to możliwość sprawdzenia, czy podczas naszej nieobecności ktoś nie zalogował się na nasze konto, a po drugie możemy weryfikować w ten sposób czas, w którym zalogowani do systemu Windows są konkretni użytkownicy, na przykład dzieci.

1 W celu sprawdzenia danych o aktywności przy logowaniu i wylogowywaniu należy kliknąć po lewej stronie na **Dzienniki systemu Windows**, **Zabezpieczenia** **A**.



2 Interesują nas wpisy oznaczone w kolumnie **Kategoria zadania** **B** jako **Logon** lub **Logoff**. Na tej podstawie jesteśmy w stanie bardzo precyzyjnie określić, kiedy, o któ-



adam13zajac@gmail.com

Aplikacja
Zabezpieczenia
Ustawienia
System
Zdarzenia przesyłane dale
Dzienniki aplikacji i usług
Subskrypcje

Sukcesy inspekcji	24.02.2022 18:46:16	Microsoft Window...	4672	Special Logon
Sukcesy inspekcji	24.02.2022 18:46:38	Microsoft Window...	4672	Special Logon
Sukcesy inspekcji	24.02.2022 18:46:38	Microsoft Window...	4672	Special Logon
Sukcesy inspekcji	24.02.2022 18:56:16	Microsoft Window...	4672	Special Logon
Sukcesy inspekcji	24.02.2022 18:56:16	Microsoft Window...	4624	Logon
Sukcesy inspekcji	24.02.2022 18:46:38	Microsoft Window...	4624	Logon
Sukcesy inspekcji	24.02.2022 18:46:16	Microsoft Window...	4624	Logon
Sukcesy inspekcji	24.02.2022 18:46:38	Microsoft Window...	4624	Logon
Niepowodzenie i...	24.02.2022 18:54:51	Microsoft Window...	5152	Filtering Platform Packet Drop
Niepowodzenie i...	24.02.2022 18:55:35	Microsoft Window...	5152	Filtering Platform Packet Drop

Zdarzenie 4624, Microsoft Windows security auditing.

Ogólne Szczegóły

Logowanie do konta zakończyło się pomyślnie.

Podmiot:
Identyfikator zabezpieczeń: SYSTEM
Nazwa konta: DESKTOP-93VD4IM$
Domena konta: WORKGROUP
Identyfikator logowania: 0x3E7

Informacje o logowaniu:
Typ logowania: 5
Ograniczony tryb administratora: -
Konto wirtualne: Nie
Token z podniesionymi uprawnieniami: Tak

Poziom personifikacji: Personifikacja

Nowe logowanie:
Identyfikator zabezpieczeń: SYSTEM
Nazwa konta: SYSTEM
Domena konta: ZARZĄDZANIE NT
Identyfikator logowania: 0x3E7
Połączony identyfikator logowania: 0x0
Nazwa konta sieciowego: -
Domena konta sieciowego: -
Identyfikator GUID logowania: {00000000-0000-0000-0000-000000000000}

Nazwa dziennika: Zabezpieczenia
Źródło: Microsoft Windows security au Zalogowano: 24.02.2022 18:46:38 **C**
Identyfikator 4624 Kategoria zadania: Logon
Poziom: Informacje Słowa kluczowe: Sukcesy inspekcji

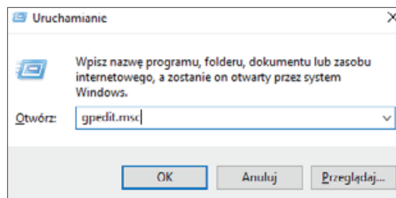
rej godzinie **C** i na jakim koncie nastąpiło zalogowanie lub wylogowanie.

3 Po kliknięciu na dany wpis na dole okna będziemy mogli sprawdzić szczegóły wpisu do dziennika.

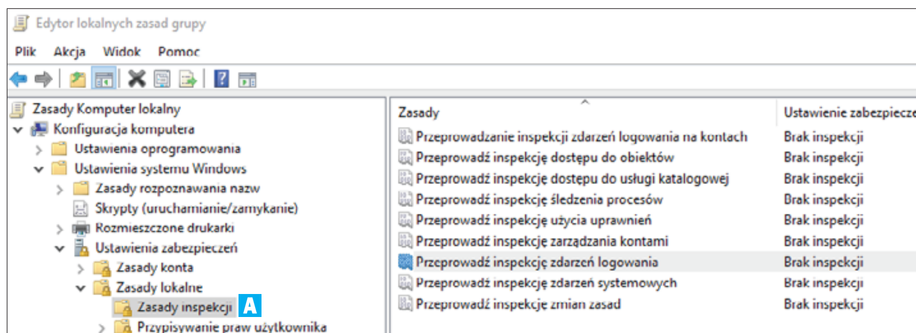
Aktywujemy wpisy o logowaniu

Jeśli w dzienniku nie widzimy wpisów tego typu, może to oznaczać, że logowanie takich zdarzeń jest zablokowane. W wyższych wersjach Windows możemy aktywować tę funkcję.

1 Wciskamy kombinację klawiszy [Win]+[R], wpisujemy **gpedit.msc** i klikamy na **OK**.

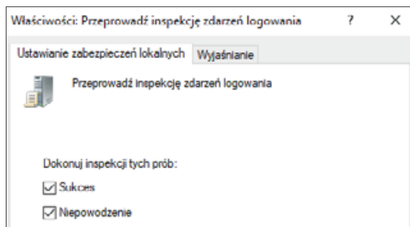


2 Następnie po lewej stronie klikamy kolejno na **Konfiguracja komputera**, **Ustawie-**



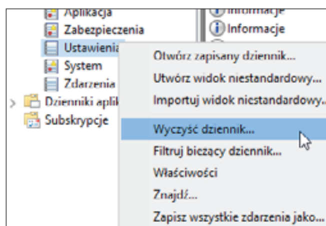
nia systemu Windows, **Ustawienia zabezpieczeń**, **Zasady lokalne**, **Zasady inspekcji** **A**. Po prawej stronie natomiast klikamy dwukrotnie na **Przeprowadź inspekcję zdarzeń logowania**.

3 Zaznaczamy opcje **Sukces** i **Niepowodzenie** i klikamy na **OK** u dołu okna. Od tej pory zdarzenia logowania będą zapisywane w dzienniku systemowym.

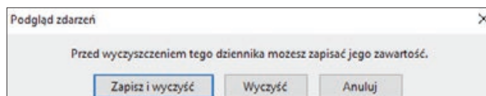


Usuwamy dane z dzienników zdarzeń

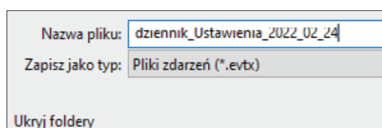
1 Klikamy prawym przyciskiem myszy w oknie po lewej stronie na wybrany dziennik, następnie z listy wybieramy opcję **Wyczyść dziennik**.



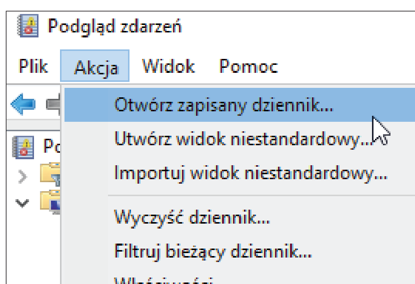
2 Jeśli chcemy zapisać dane do późniejszej diagnostyki w przypadku wystąpienia problemów, wybieramy opcję **Zapisz i wyczyść** (jeżeli wolimy niczego nie zachowywać, po prostu klikamy na **Wyczyść**).



3 Zapisujemy plik z dziennikiem na dysku, a w podglądzie zdarzeń dziennik zostanie wyczyszczony.



4 Zapisany dziennik możemy w każdej chwili otworzyć, klikając na **Akcja**, **Otwórz zapisany dziennik**.



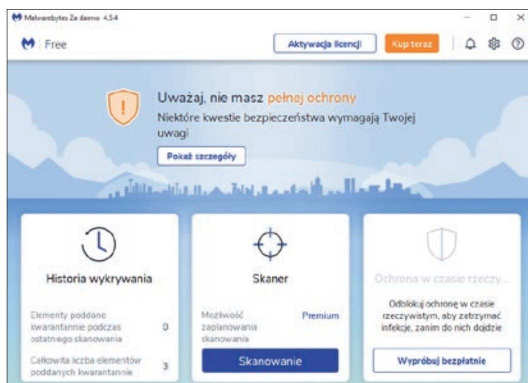
Wykrywamy narzędzia i programy wykradające nasze dane

Bardzo dużym zagrożeniem dla naszej prywatności są złośliwe programy zainstalowane w komputerze oraz ukryte wirusy, które zbierają informacje na nasz temat i wysyłają je do internetu. Mogą to być keyloggery, które zapisują wciskane klawisze, aplikacje wyświetlające reklamy i oferujące instalowanie płatnych usług i wiele innych uciążliwych lub niebezpiecznych aplikacji. Zdarza się, że pomimo ochrony programu antywirusowego takie szkodniki przedostają się na dysk. Najlepiej zainstalować specjalny program do usuwania tego typu oprogramowania – na przykład **Malwarebytes**. Możemy go pobrać z **KŚ+**.

adam13zajac@gmail.com

Walka ze szkodliwym oprogramowaniem

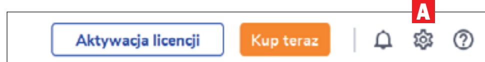
Malwarebytes to specjalny program, którego zadaniem jest wykrywanie niebezpiecznego, złośliwego oprogramowania. Dotyczy to rootkitów, trojanów i wielu innych zagrożeń. Ważną dodatkową opcją jest również wykrywanie aplikacji typu **PUP**, czyli potencjalnie niepożądanych programów – teoretycznie działają one normalnie, jednak mogą zagrażać wygodzie i bezpieczeństwu użytkownika przez oferowanie reklam i zbieranie informacji na jego temat. Obsługa Malwarebytes jest bardzo prosta. Wystarczy przeskanować komputer raz na tydzień, żeby zadbać o bezpieczeństwo.



Ustawiamy skaner

1 Instalujemy i uruchamiamy program Malwarebytes.

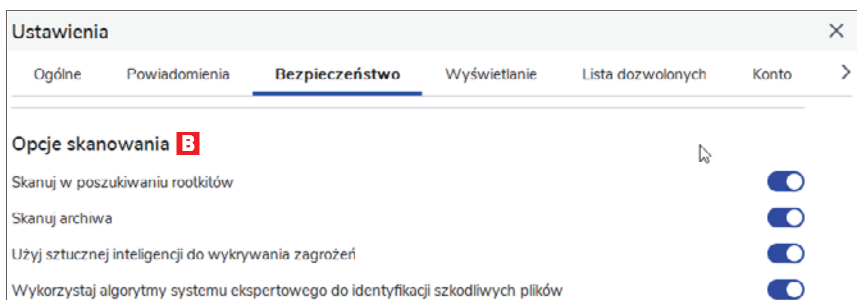
2 W głównym oknie klikamy w górnym prawym rogu na ikonę ustawień **A**.

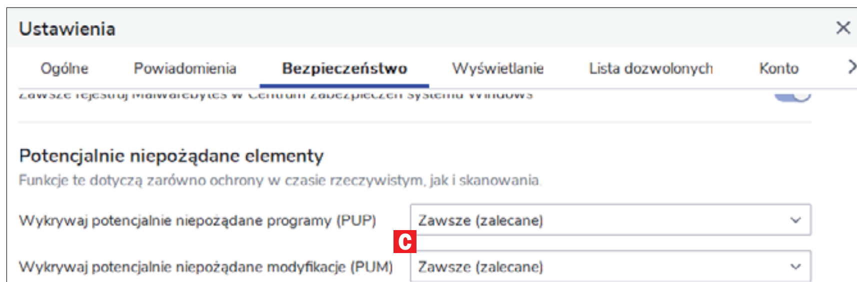


3 Przechodzimy do zakładki **Bezpieczeństwo**, a potem przewijamy widok i włączamy wszystkie opcje w sekcji **Opcje skanowania** **B**.

4 Następnie przewijamy widok do sekcji **Potencjalnie niepożądane elementy** i wybieramy dla obydwu ustawień opcję **Zawsze** **C**.

5 Taka konfiguracja pozwoli nam najskuteczniej wykrywać zagrożenia na naszym komputerze.



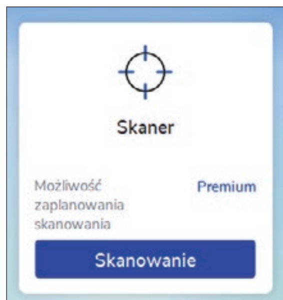


adam13zajac@gmail.com

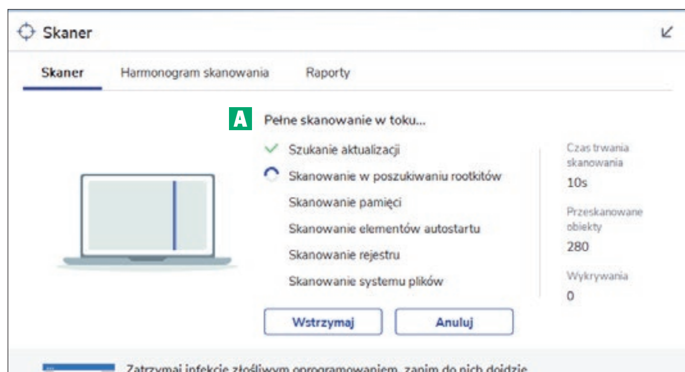
Korzystamy ze skanera

1 Upewniamy się, że mamy aktywne połączenie z internetem, które jest niezbędne do pobrania najnowszych sygnatur zagrożeń.

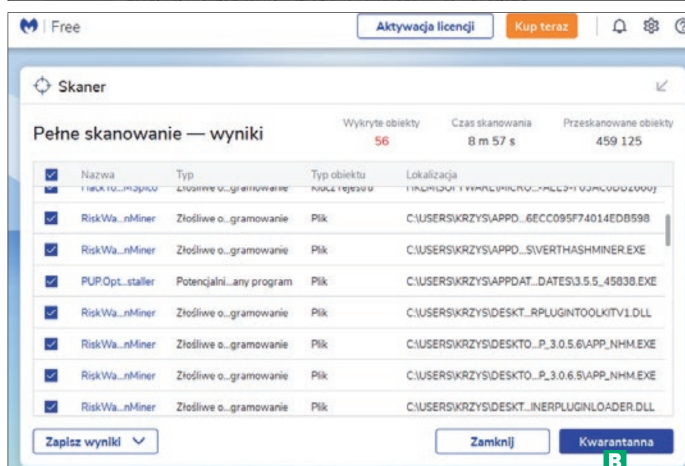
2 W głównym oknie interfejsu **Malwarebytes** klikamy na **Skanowanie**.



3 Rozpocznie się skanowanie **A**, które może potrwać bardzo długo w zależności od rozmiaru naszych dysków.



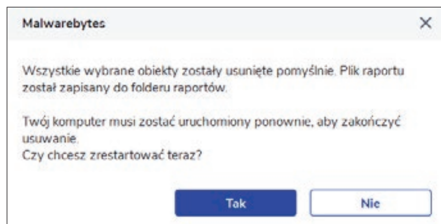
4 Na koniec zostanie przedstawiony raport ze znalezionymi zagrożeniami. Możemy sami sprawdzić zidentyfikowane obiekty. Aby przejść dalej, klikamy na **Kwarantanna** **B**. Dzięki temu nie będziemy dłużej zagrożeni.



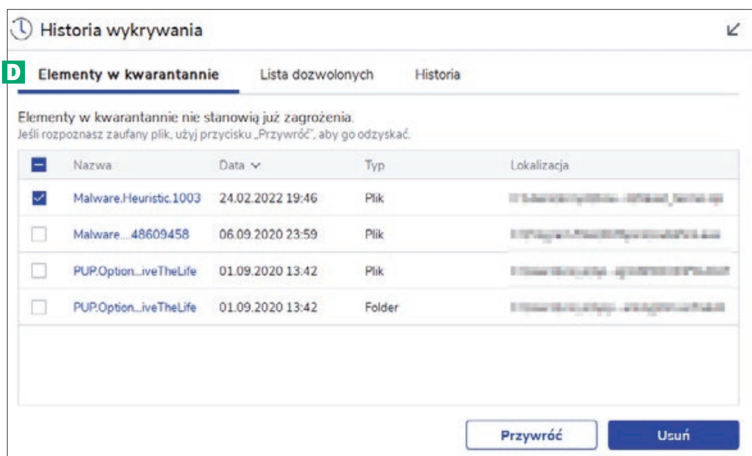
5 Jeśli nie zaznaczyliśmy jakiegoś wyszukanego obiektu, zostaniemy zapytani, czy chcemy zawsze go ignorować, czy tylko tym razem **C**. Klikamy na opcję, która nam odpowiada.



6 W większości przypadków, aby przenieść zagrożenie do kwarantanny, wymagane będzie ponowne uruchomienie komputera. Klikamy na **Tak**.



adam13zajac@gmail.com



7 Po ponownym uruchomieniu komputera włączamy program Malwarebytes i przechodzimy do zakładki **Historia wykrywania**, a następnie klikamy na **Elementy w kwarantannie** **D**.

8 Znajdziemy tu wszystkie zagrożenia, możemy teraz ostatecznie podjąć decyzję o neutralizacji zagrożenia poprzez wybranie go i kliknięcie na **Usuń** w prawym dolnym rogu.

Czyścimy plik wymiany przy zamykaniu komputera

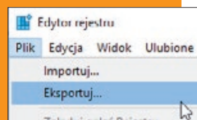
Plik wymiany przechowywać może bardzo wiele informacji dotyczących naszej ostatniej sesji. Można go odczytać i odkryć, nad czym ostatnio pracowaliśmy i jakie pliki były otwierane. Dla zwiększenia bezpieczeństwa i ochrony prywatności możemy skonfigurować system tak, aby czyścił zawartość tego pliku przy zamykaniu. Plik wymiany, czy też stronicowania, służy w systemie Windows jako rozszerzenie pamięci RAM. Jeśli mamy jej zbyt mało, dane zapisywane są na naszym dysku właśnie w pliku wymiany, który jest traktowany jako wirtualny RAM. Dzięki temu komputer nadal pracuje w miarę stabilnie bez zawieszania się, możemy jednak odczuć spowolnioną pracę dysku, który będzie w ciągłym użyciu. Wszelkie dane zapisane w pamięci RAM są automatycznie usuwane przy wyłączaniu zasilania – gdy kości pamięci nie mają zasilania, przechowywane dane zostają zapomniane. W przypadku pliku stronicowania jest jednak inaczej. Dostęp do zapisanych danych jest bardzo prosty i nie są one domyślnie czyszczone. Możemy sami skonfigurować system Windows do czyszczenia tego pliku przy każdym zamknięciu systemu, co zwiększy nasze bezpieczeństwo i uniemożliwi sprawdzenie naszej aktywności w ostatniej sesji. Wadą takiego rozwiązania jest możliwe spowolnienie czasu zamykania systemu. Z drugiej jednak strony będziemy mogli zaobserwować minimalne zredukowanie czasu potrzebnego na rozruch. A w większości przypadków istotny jest raczej czas startu komputera, a nie jego zamknięcia.

adam13zajac@gmail.com

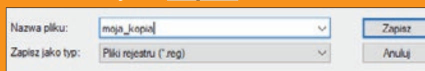
TWORZYMY I PRZYWRACAMY KOPIĘ ZAPASOWĄ REJESTRU

Zawsze przed rozpoczęciem wprowadzania jakichkolwiek zmian w rejestrze naszego systemu należy wykonać pełną kopię zapasową. Jeśli niespodziewanie w trakcie wprowadzania zmian wystąpi choćby na przykład nagła przerwa w zasilaniu, będziemy mogli szybko przywrócić rejestr do poprzedniego stanu.
Warto też wiedzieć, że podczas tworzenia punktu przywracania systemu zapisywana jest w nim aktualna kopia rejestru.
Oto jak tworzyć i przywracać kopię zapasową rejestru.

1 Uruchamiamy **Edytor rejestru**, a następnie klikamy na górnym pasku na **Plik**, **Eksportuj**.



2 Podajemy nazwę pliku kopii zapasowej i klikamy na **Zapisz**.

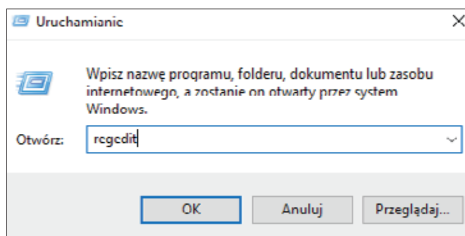


3 W celu przywrócenia kopii wystarczy, że klikniemy na **Plik**, **Importuj** i wskażemy plik z kopią.

Wprowadzamy zmiany

1 Wciskamy jednocześnie klawisze Win+R.

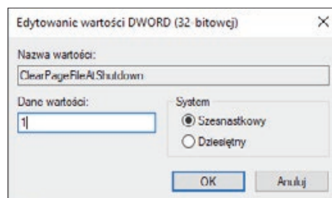
2 W oknie **Uruchamianie** wpisujemy **regedit** i klikamy na **OK**. Musimy również potwierdzić uprawnienia administratora.



3 Następnie przechodzimy do klucza: **Komputer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**

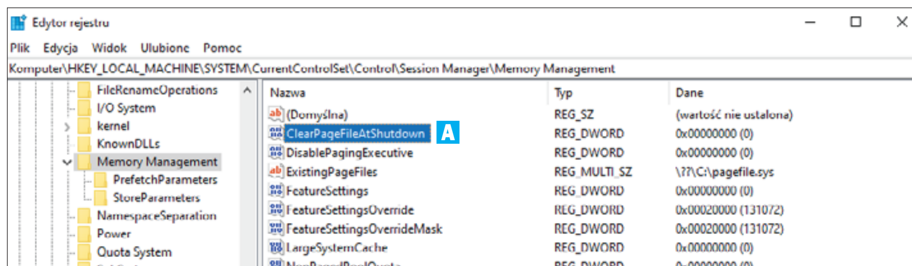
4 Teraz w prawym panelu klikamy dwukrotnie na wartość: **ClearPageFileAtShutdown** **A**.

5 Zmieniamy domyślne dane wartości z 0 na **1** i klikamy na **OK**.



6 Od teraz przy zamykaniu systemu plik wymiany będzie czyszczony automatycznie.

W każdej chwili możemy cofnąć zmiany, powtarzając kroki tej porady i podając w danych wartości **0** zamiast 1.



adam13zajac@gmail.com

4 Bezpieczeństwo i znikanie z internetu

Mówi się, że jeśli coś raz trafiło do internetu, pozostaje w nim już na zawsze. Oczywiście często jest to prawda, jednak możemy podjąć odpowiednie kroki w celu zadbania o to, aby nasze dane do internetu nie trafiły. W tym rozdziale zajmiemy się między innymi szyfrowaniem Windows i kontrolą ruchu sieciowego na naszym urządzeniu. Przeczytamy też, jak zniknąć z internetu

Szyfrowanie systemu Windows

Zanim przejdziemy do usuwania naszych danych i znikania z sieci, warto zabezpieczyć system przed osobami trzecimi. Najlepszą ochroną prywatności jest zabezpieczenie dysku poprzez wprowadzenie szyfrowania. Nawet jeśli nasz laptop zostanie skradziony lub ktoś będzie chciał uzyskać dostęp do danych na dysku bez naszej wiedzy, będzie to praktycznie niemożliwe. Jedyna słabość takiego rozwiązania to tylko i wyłącznie błąd ludzki – na przykład gdy przez przypadek powiemy komuś, jakie mamy hasło, lub zapiszemy je na kartce, żeby nie zapomnieć, i osoby postronne je poznają. W innym przypadku nie ma szans na złamanie odpowiednio długiego i mocnego hasła.

Szyfrować foldery czy cały dysk?

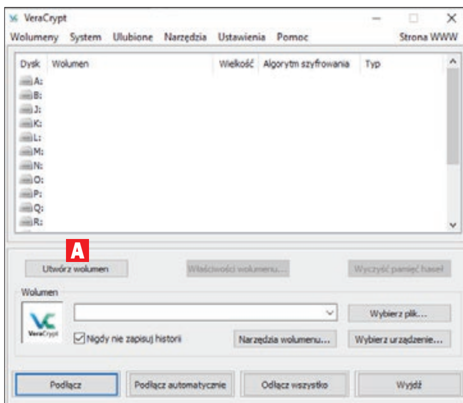
Z punktu widzenia bezpieczeństwa zalecane jest szyfrowanie całego dysku. Może się to jednak wiązać ze spadkiem wydajności dysku w zależności od jego rodzaju. Jeśli korzystamy z szybkiego nośnika SSD, zmiana nie powinna negatywnie wpłynąć na komfort korzystania z komputera. W przypadku mało wydajnych dysków twardych może to stanowić utrudnienie. W takim wypadku, jeżeli zależy nam na wydajności i nie mamy potrzeby szyfrowania całego nośnika, możemy za pomocą programu **VeraCrypt** utworzyć specjalny magazyn, który będzie obejmować wybrany plik lub nawet partycję.

Szyfrowany wolumen w VeraCrypt

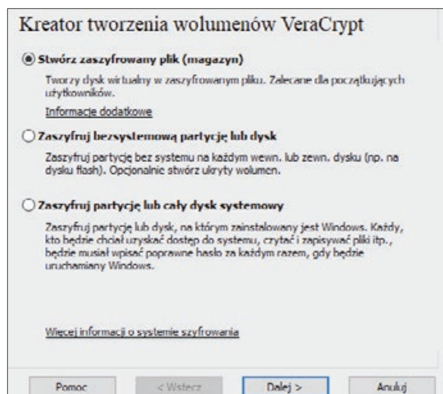
1 Po zainstalowaniu **VeraCrypt** (**DVD-KOD: 032/033** 32-/64-BIT) uruchamiamy program.

2 W jego oknie musimy kliknąć na **Utwórz wolumen** **A**.

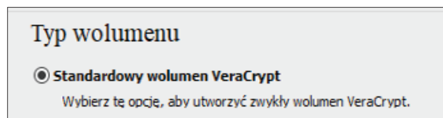
adam13zajac@gmail.com



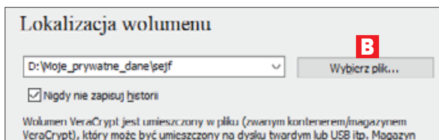
3 Pozostawiamy wybraną domyślnie opcję **Stwórz zaszyfrowany plik** i klikamy na **Dalej**.



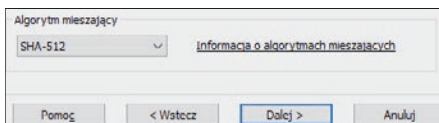
4 Następnie wybieramy opcję **Standardowy wolumen VeraCrypt** i klikamy na **Dalej**.



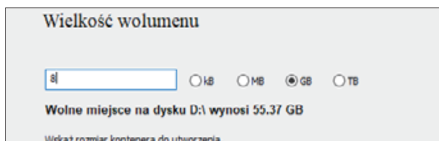
5 Teraz klikamy na **Wybierz plik** **B**, musimy podać nazwę naszego wolumenu i jego lokalizację. **Uwaga!** Nie wybierajmy istniejącego pliku, gdyż zostanie on skasowany – pliki do zaszyfrowania przenosimy do wolumenu dopiero po jego utworzeniu.



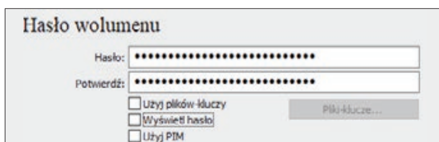
6 Pozostawiamy ustawienia algorytmów szyfrujących i mieszania bez zmian i klikamy na **Dalej**.



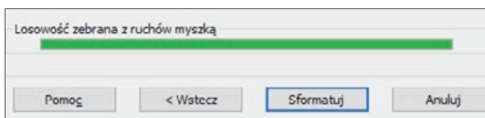
7 Teraz podajemy rozmiar wolumenu. **Uwaga!** Zwróćmy uwagę na jednostki, w których podajemy dane. Po wpisaniu wartości klikamy na **Dalej**.



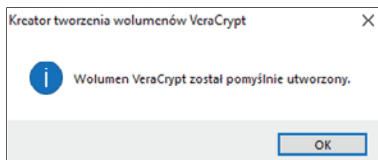
8 Następnie wpisujemy hasło, które będzie chroniło nasz wolumen. Rekomendowane jest hasło o długości przynajmniej 20 znaków. Najlepiej, jeśli będzie zawierało także przynajmniej jedną dużą literę, cyfrę i znak specjalny.



9 W kolejnych krokach musimy określić, czy będziemy przechowywać pliki większe niż 4 GB. Jeśli tak, wybieramy system plików exFAT lub NTFS. Musimy również wykonywać losowe ruchy myszą w celu poprawy kryptograficznej jakości generowanych kluczy. Dopiero gdy pasek dojdzie do końca, klikamy na **Sformatuj**.

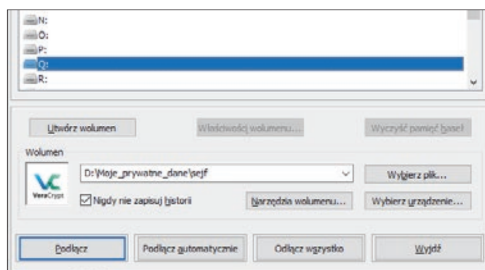


10 Po utworzeniu wolumenu klikamy na **OK**.

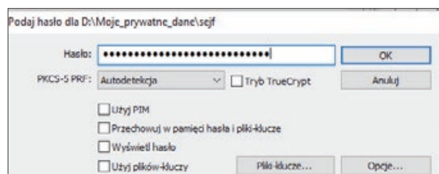


Korzystamy z wolumenu

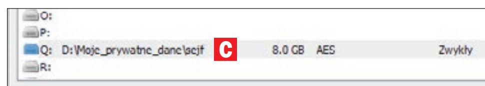
1 W głównym oknie programu VeraCrypt klikamy na **Wybierz plik**. Wybieramy nasz wolumen i literę dysku, a następnie klikamy na **Podłącz**.

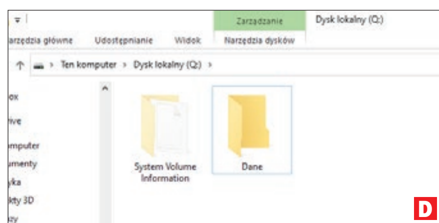


2 Podajemy hasło i klikamy na **OK**.



3 Po udanej weryfikacji nasz zasób zostanie dodany jako „nowy dysk" **C** i będziemy





BITLOCKER CZY VERACRYPT

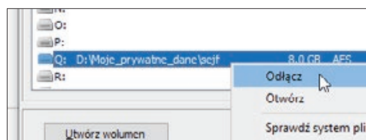
Jeśli używamy Windows 10 lub 11 w wersji Pro, Enterprise lub Education, możemy skorzystać z dostępnej systemowo opcji szyfrowania dysku BitLocker. Wymaga ona modułu TPM. Jeżeli nasz komputer go nie ma, będziemy musieli skorzystać z dodatkowego nośnika, na przykład z pendrive'a.

Zabezpieczony dysk będzie całkowicie bezpieczny w przypadku zwykłego ataku. Prośba o autoryzację pojawia się, zanim zostanie załadowany system.

Warto jednak rozważyć skorzystanie z programu VeraCrypt. Oferuje on bardzo podobne rozwiązanie, a jest ono nawet uważane za bezpieczniejsze. Największa różnica polega na tym, że BitLocker to funkcja systemu. Microsoft może mieć specjalny algorytm do odblokowania zasobów zaszyfrowanych BitLockerem. W przypadku VeraCrypt mamy do czynienia z otwartym oprogramowaniem, które przeszło wiele audytów bezpieczeństwa i wydaje się nie mieć wad w kodzie.

Dodatkowo VeraCrypt pozwala nam na zaszyfrowanie wybranej przestrzeni dysku, a nie całej jego powierzchni.

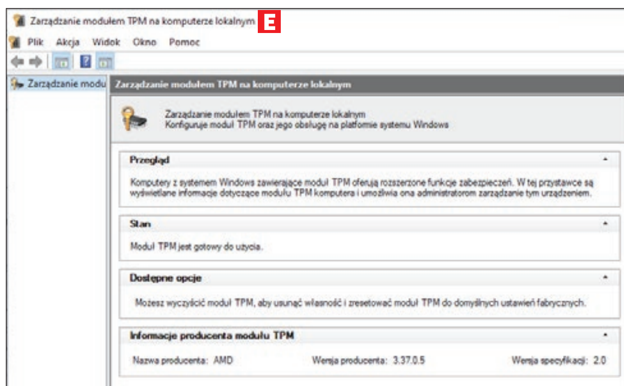
mogli korzystać z niego zupełnie normalnie, przez Eksplorator **D** – kopiując pliki, zapisując itp. Po zakończeniu pracy z wolumenem w VeraCrypt klikamy na niego prawym przyciskiem myszy i z menu wybieramy opcję **Odłącz**.



Czy nasze urządzenie ma moduł TPM

By sprawdzić, czy nasz komputer ma moduł TPM, naciskamy [Win]+[R]. W nowym oknie wpisujemy **tpm.msc** i klikamy na **OK**. Jeżeli nasze urządzenie jest wyposażone w moduł TPM, pojawi się okno z informacjami o tym

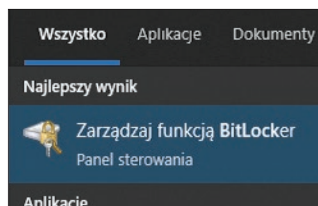
adam13zajac@gmail.com

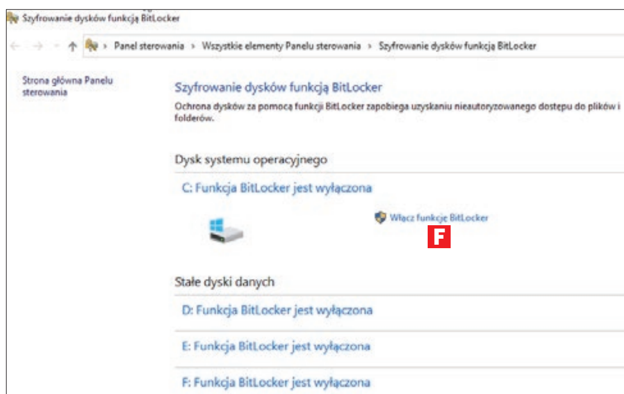


układzie **E**. Jeśli nie mamy takiego modułu, system wyświetli informację, że nie może odnaleźć układu.

Korzystamy z BitLockera

1 W wyszukiwarkę systemową wpisujemy **BitLocker** i klikamy na znalezioną funkcję.

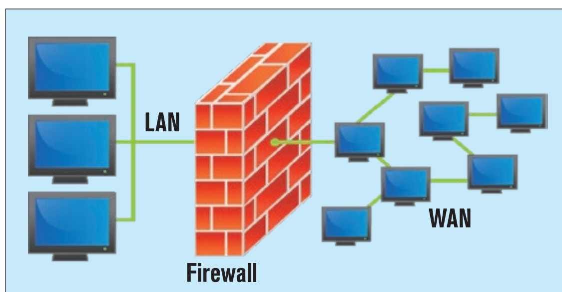




2 Klikamy na **Włącz funkcję BitLocker** **F** przy wybranym dysku, który chcemy zabezpieczyć. Postępujemy zgodnie z instrukcjami kreatora. Jeśli nasz komputer nie jest wyposażony w moduł TPM, musimy przygotować pendrive.

Blokujemy ruch sieciowy dla podejrzanych aplikacji

W systemie Windows mamy dostęp do różnego rodzaju rozwiązań, które pozwalają na blokowanie ruchu sieciowego, jednak nie są one najłatwiejsze w obsłudze. Dlatego warto poznać specjalne programy, które pozwolą w chwilę przejąć kontrolę nad naszym firewallem i zablokować ruch sieciowy dla wybranych aplikacji.



Firewall (ściana ognia) to inaczej po prostu zapora sieciowa. Istnieją zapory sprzętowe oraz programowe. Ich głównym zadaniem jest blokada niepowołanego dostępu do naszej sieci lub komputera z internetu. Firewall głównie realizuje kilka zadań: filtrowanie pakietów, sprawdzanie identyfikacji użytkowników, zabezpieczanie programów pra-

adam13zajac@gmail.com

cujących z protokołami sieciowymi. Wszelkie incydenty bezpieczeństwa są rejestrowane w specjalnych logach, które można później analizować.

Prezentowane w tym rozdziale programy w ogromnym stopniu ułatwiają korzystanie z wbudowanych w Windows narzędzi do ochrony. Dają nam bardzo prosty dostęp do zarządzania ruchem sieciowym na naszej maszynie. W kilka kliknięć możemy zablokować dostęp do sieci dla konkretnego procesu lub też zmienić stopień automatycznej ochrony. Możemy również tworzyć białe oraz czarne listy, które zawierają procesy, którym ufamy, oraz takie, które mają być zawsze blokowane. Dodatkowo będziemy w stanie namierzyć, z jakiego adresu IP wychodzi ruch, który może powodować problemy na naszym komputerze, i ile transferu danych w tle zużywa jakaś aplikacja. Wszystkie porady opierają się na aplikacjach **Portmaster** (DVD-KOD: 034) z płyty dołączonej do książki oraz **GlassWire** dostępnej w KŚ+ (ksplus.pl).

Monitorowanie ruchu – GlassWire

To jeden z najlepszych programów do monitorowania i analizy ruchu sieciowego na komputerze. Ma możliwość automatycznego lub ręcznego blokowania dostępu do internetu wybranym aplikacjom, a nawet usługom. Umożliwia weryfikację, z jakim hostem się łączymy, oraz podaje dokładny adres IP docelowego hosta. W prosty sposób możemy też sprawdzić, ile transferu danych wykorzystuje konkretna aplikacja. Interfejs programu jest dość nowoczesny i łatwy w obsłudze. Dodatkowo program, pracując w tle, wyświetla powiadomienia za każdym razem, gdy nowa aplikacja lub proces chce uzyskać dostęp do sieci, dzięki czemu żadna usługa nie uzyska do niej dostępu bez naszej wiedzy.

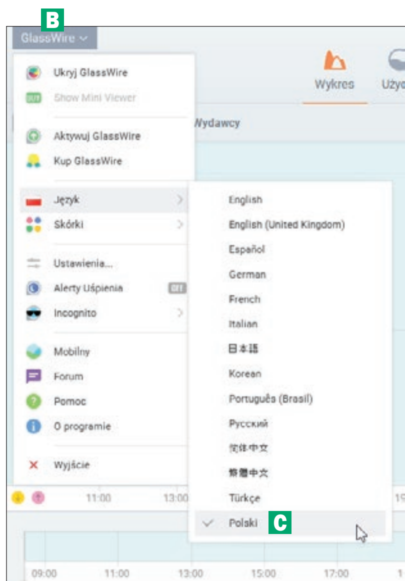
Pierwsze kroki

1 Po zainstalowaniu i uruchomieniu GlassWire w głównym oknie pojawi się widok wykresu w trybie **Wszystkie** **A**. Są tu widoczne w czasie rzeczywistym wszystkie dostępy do sieci i ogólny ruch sieciowy.

2 Domyślnie program uruchomiony zostanie w języku angielskim. W celu zmiany języka musimy kliknąć w górnym lewym rogu na **GlassWire** **B**, **Language**, **Polski** **C** i ponownie uruchomić program.



adam13zajac@gmail.com

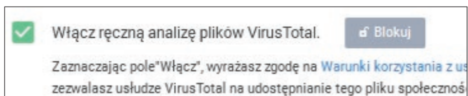


Weryfikujemy ruch sieciowy

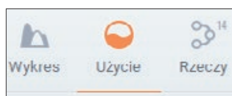
1 Najpierw przechodzimy do ustawień programu, klikamy na **VirusTotal**, a następnie po prawej stronie na **Odblokuj** **D**



i zaznaczamy opcję **Włącz ręczną analizę plików VirusTotal**.

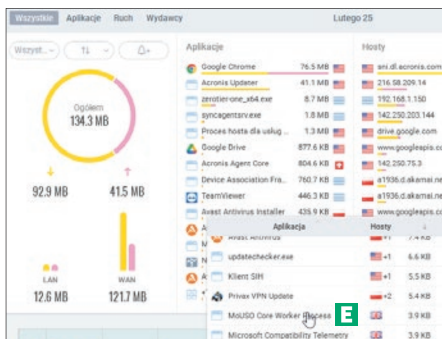


2 Na górnym pasku przechodzimy do zakładki **Użycie**.

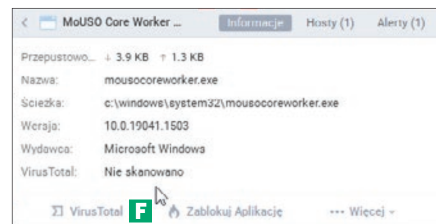


3 Tutaj możemy sprawdzić, jak duży ruch sieciowy generują poszczególne aplikacje i usługi. Dodatkowo, jeśli nie znamy jakiegoś procesu, możemy dokładnie zweryfikować, gdzie na naszym komputerze znajduje się plik wykonywalny tego procesu.

4 Aplikacje wyświetlane są kolejno od tych, które wykorzystują najwięcej transferu, do tych, które go prawie nie zużywają. Warto sprawdzić również te ukryte w polu **+ więcej** – najeżdżamy kursorem na to pole, a następnie klikamy na proces **E**, który chcemy zweryfikować.



5 Po kliknięciu pojawią się szczegółowe informacje dotyczące danego procesu. Możemy dowiedzieć się dokładnie, gdzie na naszym dysku jest zapisany plik wykonywalny. Jeśli nie wiemy, czy możemy zaufać danemu procesowi, klikamy na **VirusTotal** **F**.



6 Po chwili pojawi się informacja z wynikiem skanowania – zielony znacznik oznacza, że proces jest bezpieczny.



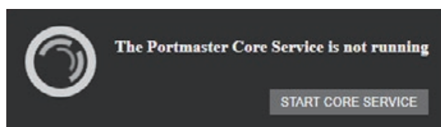
adam13zajac@gmail.com

Aktywność sieciowa komputera – Portmaster

GlassWire jest świetnym narzędziem, niestety w pełnej wersji jest płatny. Dlatego też do blokowania połączeń warto korzystać z **Portmastera**. Jest to nowe, darmowe narzędzie open source do monitorowania całej aktywności sieciowej komputera. Portmaster wykrywa łączenie się zainstalowanych programów z internetem i wyświetla wszystkie uruchomione procesy ze szczegółowymi informacjami o każdym połączeniu. Do dyspozycji mamy funkcję ręcznego zezwalania na połączenia lub ich blokowania, która pozwala odciąć od internetu wybrane programy i procesy systemowe. Jest też funkcja automatycznego blokowania na podstawie wybranych list filtrów. Są ustawienia globalne i dla poszczególnych aplikacji oraz konfigurowalne ustawienia dla różnych sieci.

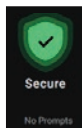
Blokujemy dostęp do sieci

1 Po uruchomieniu Portmastera klikamy w głównym oknie na **Start Core Service**.

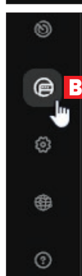


2 Po chwili automatycznie zostanie uruchomione narzędzie do monitorowania **A** wraz z filtrami.

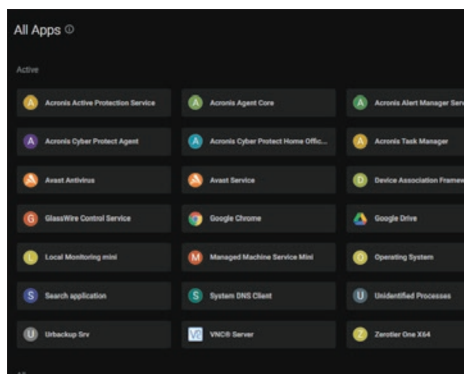
3 Z programu możemy zacząć korzystać, gdy po lewej stronie pojawi się symbol zielonej tarczy.

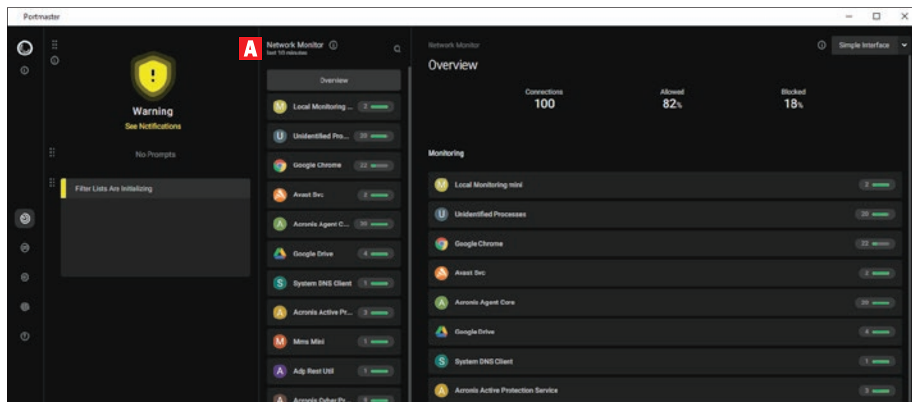


4 Domyślny widok, w którym jesteśmy, to **Network Monitor**, gdzie możemy w czasie rzeczywistym obserwować, co dzieje się na naszym urządzeniu. W celu zablokowania dostępu dowolnej aplikacji klikamy na pasku po lewej stronie na **Per-App Settings** **B**.



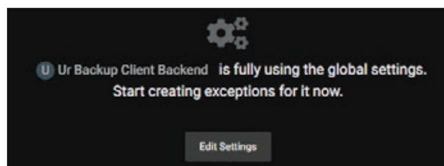
5 Teraz w oknie po prawej stronie możemy wyszukać dowolną aplikację na naszym urządzeniu, która w trakcie pracy programu uzyskała dostęp do internetu. Jeśli chcemy zablokować jej dostęp, klikamy na nią.



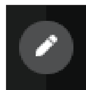


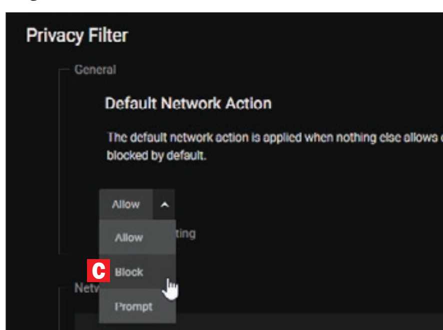
adam13zajac@gmail.com

6 Następnie u dołu okna klikamy na **Edit Settings**.



7 W kolejnym oknie klikamy na ikonę długopisu przy opcji **Default Network Action**.





8 Klikamy na **Allow** i zmieniamy wartość na **Block** C. Od tego momentu cały ruch sieciowy danej aplikacji będzie blokowany.

Usuwanie kont w popularnych serwisach

Ze względu na zachowanie prywatności warto wiedzieć, w jaki sposób można usunąć lub dezaktywać konta w popularnych serwisach społecznościowych. Poniżej przeczytamy, jak to zrobić, na przykładzie tych, z których korzysta się najczęściej. Oczywiście tego typu serwisy często zmieniają układ swojego menu i ustawień, jednak opierając się na opisanych krokach, powinniśmy nawet w wypadku takich zmian skutecznie usunąć lub dezaktywować konto w danym serwisie.

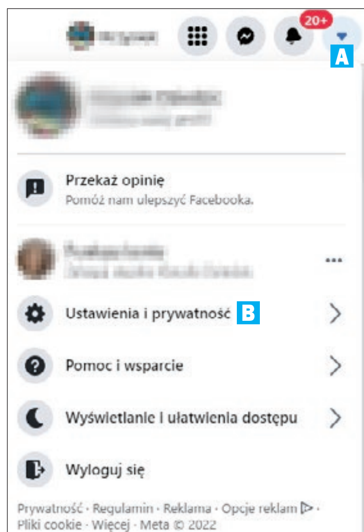
Facebook

To zdecydowanie najpopularniejszy w Polsce serwis społecznościowy. Możemy umieszczać w nim różnego typu informacje, komunikować się ze znajomymi, przesyłać pliki. Korzystając z niego, zgadzamy się jednak na wyświetlane nam reklamy, tworzenie spersonalizowanego profilu reklamowego, sprzedaż zebranych o nas informacji do firm trzecich itp. Co warte uwagi, aplikacje na smartfony z grupy Facebooka: Facebook, Messenger, Instagram – to aplikacje, które zbierają najwięcej informacji o użytkownikach.

Dezaktywacja

Jest to standardowe rozwiązanie w przypadku Facebooka. Możemy dezaktywować konto, usuwając tym samym naszą nazwę profilu, imię, nazwisko oraz zdjęcia z większości udostępnianych treści. Niektóre treści nadal mogą być jednak widoczne dla użytkowników serwisu.

1 Logujemy się na nasze konto Facebook, a następnie klikamy na strzałkę A w górnym prawym rogu i z menu wybieramy opcję **Ustawienia i prywatność** B, a następnie klikamy na **Ustawienia**.



adam13zajac@gmail.com

FACEBOOK A ODEJŚCIE BLISKICH

Konta w serwisie Facebook nie są zawieszane automatycznie i teoretycznie pozostają aktywne na zawsze. Jeśli jednak ktoś z naszych bliskich odejdzie, w większości przypadków chcielibyśmy, żeby jego konto zostało usunięte lub miało status **In memoriam**, który jest przeznaczony dla kont osób, których już z nami nie ma. Możemy sami wystąpić z prośbą do serwisu Facebook o zmianę statusu konta bliskiej osoby lub o usunięcie takiego konta. Nie musimy posiadać hasła dostępu do takiego konta.

1 Po zalogowaniu się do naszego konta wchodzimy na adres: **https://www.facebook.com/help/contact/228813257197480**.

2 Pojawi się specjalny wniosek, który należy dokładnie wypełnić. Potrzebne do weryfikacji będą również skany dokumentów, które należy przesłać.

3 Do potwierdzenia naszych uprawnień będzie konieczne posiadanie jednego z dokumentów: pełnomocnictwo, akt urodzenia, ostatnia wola i testament, oświadczenie o powołaniu na zarządcę

Wniosek specjalny dotyczący konta ubezwłasnowolnionej lub zmarłej osoby

Przykro nam z powodu Twojej straty. Dokładamy wszelkich starań, aby Twoje zgłoszenie zostało zweryfikowane. Prosimy pamiętać, że w związku z pandemią koronawirusa (COVID-19) mamy teraz mniej weryfikatorów zgłoszeń, co oznacza, że możemy potrzebować dodatkowego czasu, aby nadać kontu status „In memoriam" albo je usunąć.

Przepraszamy i składamy wyrazy współczucia z powodu Twojej straty. Więcej aktualnych informacji na temat przesyłania wniosków o nadanie statusu „In memoriam" oraz usunięcie konta znajdziesz w Centrum pomocy. »

Skorzystaj z tego formularza, żeby złożyć wniosek o usunięcie konta osoby ubezwłasnowolnionej z przyczyn zdrowotnych lub zmarłej albo aby przesłać prośbę o nadanie specjalnego statusu „In memoriam".

Składamy kondolencje i dziękujemy za cierpliwość i wyrozumiałość podczas trwania tej procedury. Pamiętaj, że na ogół nie odpowiadamy na zgłoszenia problemów innych niż związane z nadaniem kontu statusu „In memoriam".

Z uwagi na ochronę prywatności użytkowników Facebooka nie możemy przekazywać nikomu danych logowania do kont.

Uwaga: Jeśli chcesz zgłosić zhakowane konto osoby żyjącej, nie wypełniaj formularza poniżej. Dowiedz się, co należy zrobić.

Twoje pełne imię i nazwisko



majątkowego. Alternatywnie nasze konto musi mieć status opiekuna zmarłej osoby.

4 W celu potwierdzenia śmierci bliskiej osoby musimy również przedstawić dokument do weryfikacji. Może być to nekrolog, karta upamiętniająca zmarłego lub akt zgonu.

5 **Uwaga!** Powinniśmy zasłonić wszelkie informacje, które nie są wymagane do weryfikacji, jak numer PESEL i inne tego typu informacje.

6 Cała procedura jest nadzorowana przez człowieka, a nie komputer, więc rozpatrzenie i realizacja naszego wniosku nie będą natychmiastowe.

2 Teraz po lewej stronie klikamy na **Twoje informacje na Facebooku** **C**.

3 Następnie klikamy po prawej stronie na **Wyświetl** **D** przy opcji **Dezaktywacja i usuwanie**.

Ustawienia

Ogólne

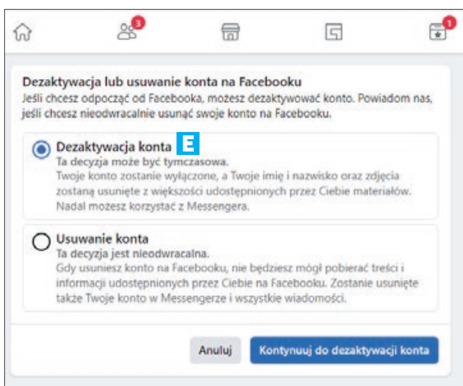
Bezpieczeństwo i logowanie

Twoje informacje na Facebooku **C**

Aktywność poza Facebookiem	Przeglądanie lub usuwanie aktywność ze stron firm i organizacji odwiedzanych poza Facebookiem.	Wyświetl
Zarządzanie Twoimi informacjami	Dowiedz się więcej o sposobie zarządzania swoimi informacjami.	Wyświetl
Dezaktywacja i usuwanie	Dezaktywuj tymczasowo lub usuń nieodwracalnie swoje konto.	**D** Wyświetl

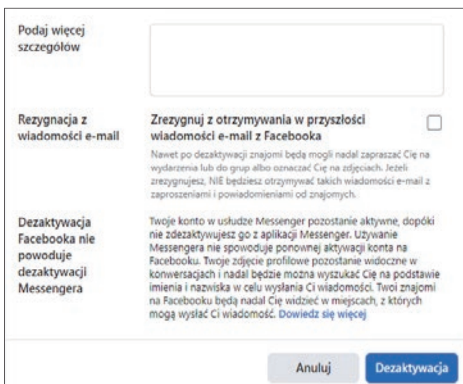
Informacje · Utwórz reklamę · Utwórz stronę · Twórcy aplikacji · Praca · Prywatność · Pliki cookie · Opcje wyświetlania reklam · Regulamin · Pomoc

adam13zajac@gmail.com



4 Następnie wybieramy opcję **Dezaktywacja konta** **E** i klikamy na **Kontynuuj do dezaktywacji konta**.

5 Teraz musimy wybrać lub podać powód dezaktywacji konta. Na koniec klikamy na **Dezaktywacja**.



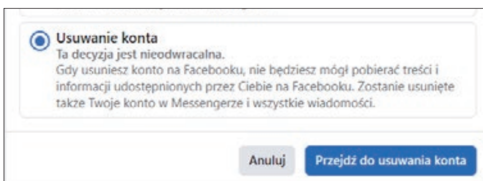
Przy tej metodzie zawieszenia konta możliwe jest jego przywrócenie.
Wystarczy po dezaktywacji ponownie się zalogować i będziemy mogli aktywować nasze konto wraz z informacjami o koncie i znajomych.

Usuwanie konta

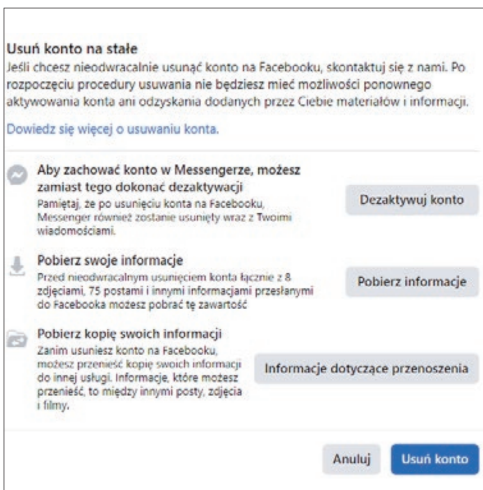
Możemy również całkowicie usunąć konto w serwisie Facebook, proces ten trwa bardzo długo (nawet do 90 dni) i nie ma możliwości jego odwrócenia.

1 Logujemy się na nasze konto w serwisie Facebook.

2 Następnie wchodzimy na stronę **https://www.facebook.com/deactivate_delete_account** i zaznaczamy opcję **Usuwanie konta** i klikamy na **Przejdź do usuwania konta**.



3 Na kolejnym ekranie klikamy po prostu na **Usuń konto**. Wbrew temu, co jest napisane na tym ekranie – mamy 30 dni na całkowite przywrócenie konta.



4 Rozpocznie się proces usuwania konta. W ciągu 30 dni mamy możliwość jego cofnięcia. Usuwanie wszystkich zdjęć i wpisów widocznych dla znajomych może potrwać jednak znacznie dłużej.

5 Aby anulować usuwanie, ponownie logujemy się na nasze konto i klikamy na **Anuluj usuwanie**.

adam13zajac@gmail.com

Twitter

Usuwanie konta z serwisu Twitter teoretycznie nie jest trudnym zadaniem. Jednak nie ma możliwości, aby usunąć je natychmiastowo. Konieczne jest dezaktywowanie konta w serwisie, a następnie nielogowanie się do niego przez ponad 30 dni. Dopiero po tym okresie konto zostanie automatycznie usunięte i nie będzie można cofnąć tego procesu. Zanim to jednak nastąpi, nasze tweety nadal będą widoczne.

To spowoduje dezaktywację Twojego konta

Proces dezaktywacji Twojego konta na Twitterze niedługo się rozpocznie. Twoja wyświetlan nazwa konta, @nazwa_użytkownika i publiczny profil nie będą już widoczne na stronie Twit ani w aplikacjach Twittera na iOS i Androida.

Co jeszcze warto wiedzieć

Możesz przywrócić swoje konto w ciągu 30 dni od dezaktywacji, jeśli dezaktywacja była przypadkowa lub nastąpiła w wyniku błędu.

Pewne informacje dotyczące konta mogą być wciąż dostępne w wyszukiwarkach takich jak Google czy Bing. Dowiedz się więcej

Jeśli chcesz zmienić @nazwę_użytkownika, nie musisz dezaktywować swojego konta. Może zmienić w ustawieniach.

Aby korzystać z tej samej @nazwy_użytkownika lub tego samego adresu e-mail na innym ko na Twitterze, zmień je przed dezaktywacją konta.

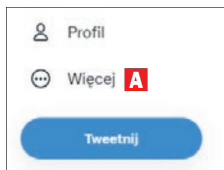
Jeśli chcesz pobrać swoje dane z Twittera, musisz wysłać wniosek i pobrać dane przed dezaktywacją konta. Nie można uzyskać linku do pobrania danych dotyczących konta, któr zostało dezaktywowane.

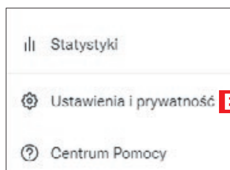
E

Dezaktywuj

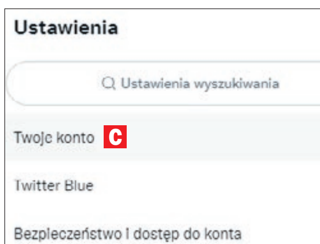
Dezaktywacja i usuwanie

1 Po zalogowaniu się na nasze konto klikamy po prawej stronie na **Więcej** **A**, a potem na **Ustawienia i prywatność** **B**.

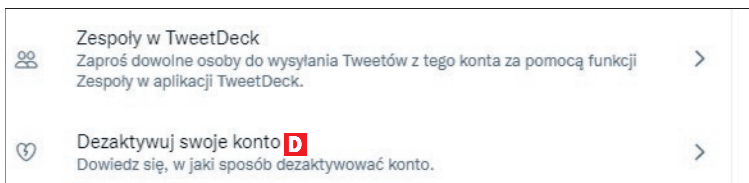




2 Teraz po lewej stronie klikamy na **Twoje konto** **C**.



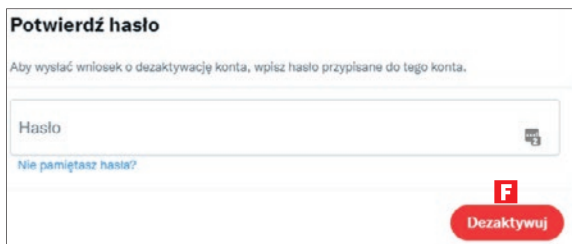
3 Po prawej stronie klikamy na **Dezaktywuj swoje konto** **D**.



4 Po zapoznaniu się z informacją dotyczącą dezaktywacji konta klikamy na **Dezaktywuj** **E**.

5 Musimy jeszcze raz podać nasze hasło i kliknąć na **Dezaktywuj** **F**.

6 Konto zostanie usunięte, jeżeli przez 30 dni nie będziemy się na nie logować.



STATUS IN MEMORIAM

Jest to specjalny status przyznawany dla konta zmarłej osoby. Konto ze statusem **In memoriam** to miejsce, w którym znajomi i rodzina mogą dzielić się ze sobą wspomnieniami o zmarłej osobie. Cechy wyróżniające konta ze statusem **In memoriam** to między innymi:

- Obok imienia i nazwiska na stronie profilu znajdują się słowa **In memoriam**.
- Znajomi mogą dzielić się wspomnieniami na osi czasu zmarłej osoby, jeśli zezwalają na to ustawienia prywatności danego konta.
- Materiały udostępnione przez zmarłą osobę (zdjęcia, posty) pozostaną na Facebooku i będą widoczne dla odbiorców, którym zostały udostępnione.
- Profile ze statusem **In memoriam** nie pojawiają się w obszarach publicznych, takich jak propozycje osób, które możesz znać, reklamy czy przypomnienia o urodzinach.
- Nie można logować się do konta ze statusem **In memoriam**.
- Nie można modyfikować kont ze statusem **In memoriam**, do których nie przypisano opiekuna konta.

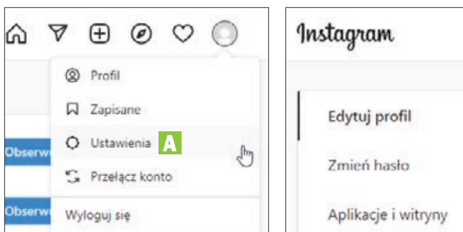
Instagram

Jest to serwis społecznościowy hostingujący zdjęcia. Został on przejęty przez Facebook w 2012 roku i od tamtej pory jest dalej rozwijany. Szybkie usunięcie konta bez wstępnej dezaktywacji jest w nim możliwe dzięki wykorzystaniu pewnej sztuczki. Jeśli planujemy nadal korzystać z tego konta w przyszłości, wystarczy zdecydować się na dezaktywację.

Dezaktywacja

1 Logujemy się na nasze konto w serwisie Instagram.

2 Klikamy na ikonę profilu w górnym prawym rogu i na **Ustawienia** A.

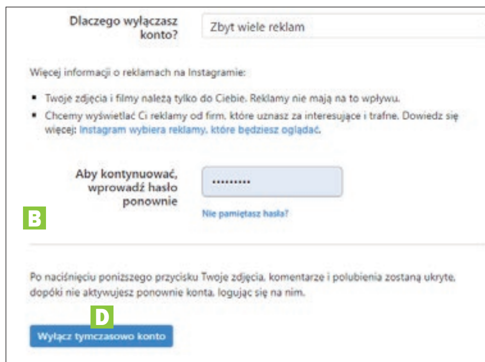


3 Następnie klikamy po lewej stronie na **Edytuj profil** B.

4 Teraz w dolnym prawym rogu klikamy na **Tymczasowe wyłączenie konta** C.



5 Następnie musimy podać powód dezaktywacji konta i nasze hasło. Dopiero wtedy będziemy mogli kliknąć na **Wyłącz tymczasowo konto** D.



6 Pozostanie ono wyłączone do czasu, aż ponownie się na nie zalogujemy. Nie zostanie ono automatycznie skasowane.

adam13zajac@gmail.com

5 Anonimowe korzystanie z internetu w praktyce

W tym rozdziale przeczytamy, jak w praktyce zachować anonimowość przy korzystaniu z internetu. Dowiemy się wszystkiego o sieci Tor, połączeniach typu VPN, szyfrowaniu e-maili oraz o szyfrowanej komunikacji. Jest to rozdział przeznaczony dla użytkowników, którzy zamierzają głównie korzystać z systemu Windows

Korzystamy z dwóch przeglądarek

Bardzo ważne w trakcie korzystania z internetu na komputerze jest stosowanie dwóch przeglądarek, nazwijmy je – bezpieczna i zwyczajna. Ta pierwsza będzie służyła nam do zapewnienia anonimowości. Zawsze, gdy będziemy chcieli odwiedzić jakąś stronę, dodać jakiś wpis na konkretnej stronie czy też wykonać inne zadanie, które wymaga dyskrecji i zachowania anonimowości, powinniśmy użyć przeglądarki, która ukryje naszą obecność w sieci. W przypadku gdy chcemy skorzystać z serwisów społecznościowych i innych usług internetowych, w których nasz adres IP i możliwość namierzenia nas nie stanowi problemu, możemy posłużyć się zwyczajną przeglądarką. Pamiętajmy o tym, aby nigdy nie używać przeglądarek bezpiecznej i zwyczajnej jednocześnie.

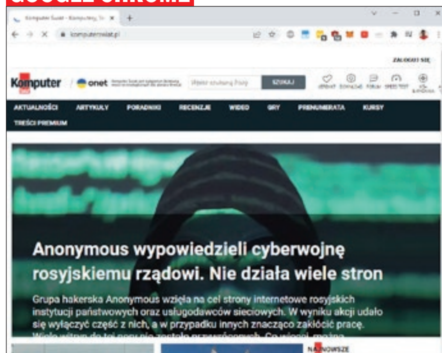
Niestety, anonimowość nie przychodzi bez ograniczeń, jednym z największych jest znacznie wolniejsze działanie przeglądarki, która jest oparta na specjalnych mechanizmach – realnie wpływają one na szybkość ładowania witryn.

Zwyczajna przeglądarka

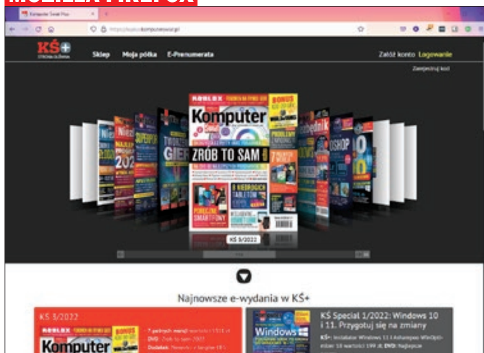
Można tutaj wymienić różne przeglądarki, jak **Google Chrome** czy **Mozilla Firefox**. Nie zapewniają one żadnych specjalnych mechanizmów maskujących naszą obecność w internecie. Ruch, który generujemy w sieci podczas korzystania z takich przeglądarek, jest łatwy do śledzenia, a nasz dostawca internetu dokładnie wie, jakie strony i kiedy odwiedzamy. Możemy z nich korzystać zawsze wtedy, gdy nie zależy nam na anonimowości.

adam13zajac@gmail.com

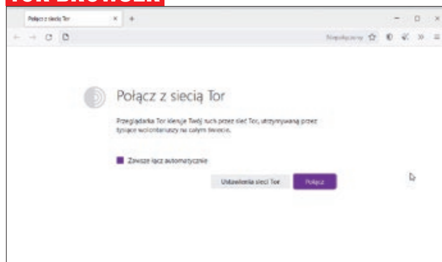
GOOGLE CHROME



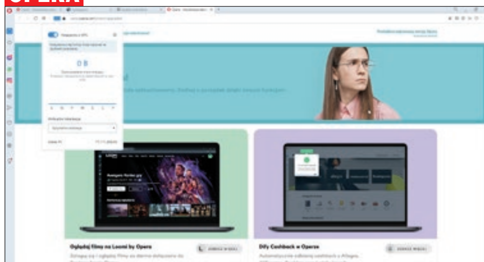
MOZILLA FIREFOX



TOR BROWSER



OPERA



Bezpieczna przeglądarka

Są to przeglądarki, które korzystają ze specjalnych mechanizmów anonimizujących, takich jak trasowanie cebulowe, VPN i innego typu rozwiązania, których głównym zadaniem jest ukrycie naszej obecności w sieci. Dobrym przykładem takiej przeglądarki jest **Tor Browser** (DVD-KOD: 055/056 32-/64-BIT) – w tym rozdziale poznamy ją dokładniej i zobaczymy, jak chroni naszą tożsamość. Warto też zwrócić uwagę na przeglądarkę Opera, która pozwala za darmo korzystać z możliwości sieci VPN (lub raczej serwera proxy) – szczegóły działania tego mechanizmu również poznamy w tym rozdziale. Jedyną w pełni bezpieczną przeglądarką jest jednak Tor Browser.

Czym jest sieć Tor i jak działa?

Jest to przykład anonimowej sieci, która podobnie jak **Freenet**, **GNUnet** czy **MUTE** – ma za zadanie chronić naszą tożsamość w internecie. Głównym celem wykorzystywania takich sieci jest chęć ominięcia narzędzi cenzury, mechanizmów filtrowania sieci i różnego typu ograniczeń w komunikacji.

Sieć Tor oparta jest na zasadzie trasowania cebulowego. Nazwa tego mechanizmu bierze się z tego, że wykorzystując kryptografię, wielowarstwowo (stąd porównanie do cebuli) szyfrowane są wszystkie przesyłane komunikaty. Przechodzą one przez ciąg różnego typu serwerów – routerów cebulowych, które nie wiedzą, jakie dane przesyłają.

Każdy może wspomóc taką sieć, uruchamiając na swoim komputerze serwer, który będzie jej służył. Prosta implementacja, jasne zasady działania i możliwość praktycznie cał-

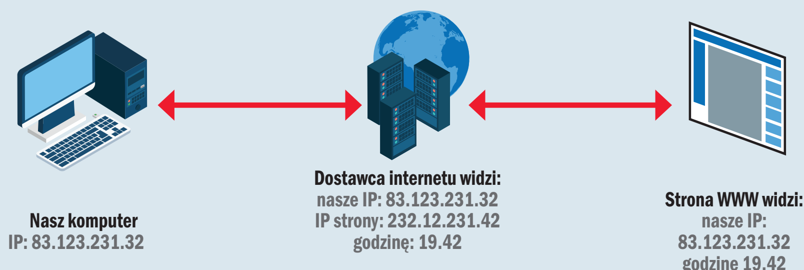
adam13zajac@gmail.com

kowitego zniknięcia w internecie to główne powody, dla których ta sieć odniosła tak duży sukces.
W teorii możliwe jest wyśledzenie użytkownika i potwierdzenie komunikacji wychodzącej z jego komputera i przychodzącej do niego, jednak wymaga ogromnych środków i zaplecza technologicznego. Takie środki stosowane są w USA, gdzie rząd może kontrolować jednocześnie węzeł początkowy i końcowy, kluczowe dla całej komunikacji. W przypadku innych państw jednak potwierdzenie wystąpienia komunikacji jest raczej niemożliwe.

Jak to działa – bez sieci Tor i z jej wykorzystaniem

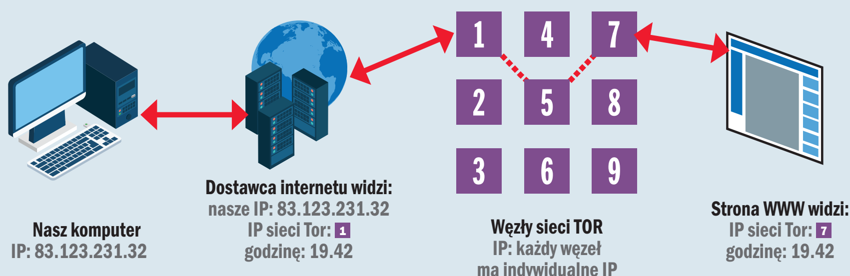
Poniższe schematy są tylko pewnym zarysem – pokazują podstawową zasadę działania. Tak

POŁĄCZENIE BEZ SIECI TOR



Inicjujemy połączenie z naszego komputera – na przykład chcemy odwiedzić stronę X. Po wpisaniu jej adresu w przeglądarce jest on rozpoznawany. Jest wysyłane żądanie dostępu do adresu IP serwera tej witryny. W tym momencie takie żądanie jest przesyłane do naszego ISP, wraz z logiem czasowym – informacją o godzinie, o której dane żądanie wyszło z danego adresu IP, oraz o tym, do jakiego IP docelowego chcemy dotrzeć. Tak więc przesyłane przez nas pakiety, nawet takie, które zawierają hasła i inne wrażliwe dane, są przechowywane na serwerach dostawców internetu.

POŁĄCZENIE Z WYKORZYSTANIEM SIECI TOR



Tutaj sytuacja wygląda zupełnie inaczej. Całe żądanie dostępu do danej witryny jest szyfrowane i przesyłane do węzła początkowego. Nasz dostawca internetu wie tylko, o której godzinie z naszego adresu został wygenerowany pakiet wychodzący, jednak nie może sprawdzić treści takiego pakietu i myśli, że ruch tego pakietu kończy się na pierwszym węźle.

adam13zajac@gmail.com

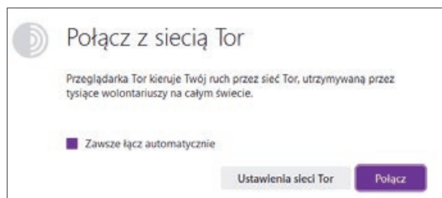
naprawdę cały proces jest znacznie bardziej skomplikowany i zawiera więcej etapów.
W rzeczywistości trasa naszego pakietu jest znacznie dłuższa i przebiega przez wcześniej ustalony pseudolosowy szereg różnego typu węzłów, co pozwala na zwiększenie bezpieczeństwa i utrudnia śledzenie.
Dopiero ostatni węzeł, czyli węzeł końcowy, otrzymuje informację pozwalającą na odszyfrowanie naszego pakietu i przesłanie go w normalny sposób do początkowego serwera. Serwer może odczytać pakiet i zna tylko czas dostępu oraz adres IP ostatniego węzła, a nie nasz.
Właśnie dzięki temu jesteśmy anonimowi, gdyż nawet dostawca internetu nie jest w stanie stwierdzić, na jakie strony wchodzimy i jakie dane przesyłamy czy pobieramy z sieci. Jedyne, co dostawca może zarejestrować, to czas dostępu i ilość transmitowanych danych niezbędnych do rozliczenia klienta.

UWAGA!

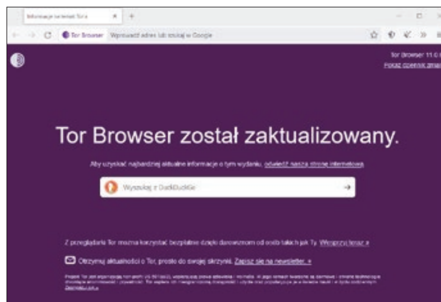
Wykorzystanie sieci anonimowej do dostępu do naszych znanych wcześniej kont jest wysoce niebezpieczne i naraża naszą anonimowość. Łatwo jest przecież wywnioskować, że to my mamy dostęp do naszego konta i zdradzić mogą nas czasy dostępu do danych serwerów.

Konfiguracja Tor Browser w Windows

Instalacja przeglądarki Tor Browser przebiega tak jak w przypadku innych programów dla systemu Windows. Przeglądarka jest dostępna w języku polskim i dodatkowo ma wbudowane rozszerzenia, które wspomagają ochronę naszego bezpieczeństwa i anonimowości, jak na przykład **NoScript**.
Przy pierwszym uruchomieniu przeglądarki pojawi się okno konfiguracyjne. W zdecydowanej większości przypadków wystarczy kliknąć na **Połącz**, aby przeglądarka rozpoczęła procedurę łączenia z siecią Tor. Jeśli jednak nasze łącze jest cenzurowane lub korzystamy z serwera proxy, wtedy musimy kliknąć na **Konfiguruj**, inaczej nie będziemy mogli korzystać z tej przeglądarki.



Pojawi się okno łączenia z siecią Tor. Na tym etapie pobierana jest lista wszystkich dostępnych węzłów, na podstawie których będzie tworzone połączenie i staniemy się anonimowi w internecie. Dodatkowo wczytywane są specjalne certyfikaty uwierzytelnienia i inne informacje niezbędne do poprawnej pracy sieci. Ten proces powinien zakończyć się bez żadnych kłopotów, jeśli jednak one się pojawią, może to oznaczać na przykład blokadę ze strony programu antywirusowego lub przez ustawienie firewalla.



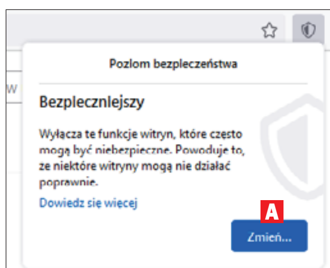
Aktualizacje

Jeśli po uruchomieniu przeglądarki pojawi się informacja, że jest ona nieaktualna, zanim zaczniemy dalsze korzystanie, priorytetem

powinno być dla nas jak najszybsze wykonanie aktualizacji. Aktualizacje eliminują błędy lub luki w zabezpieczeniach. W sytuacji gdy od funkcjonalności tej przeglądarki zależy nasza anonimowość, nie możemy sobie pozwolić na narażanie się na niebezpieczeństwo przez odkładanie aktualizacji. **Domyślnie przeglądarka przy starcie sama sprawdza, czy jest dostępna nowa wersja oprogramowania, i informuje nas o tym na stronie głównej.**

Wybieramy poziom bezpieczeństwa

Zanim zaczniemy korzystać z przeglądarki, ważne jest wybranie odpowiedniego dla nas poziomu bezpieczeństwa. Chodzi po prostu o ustalenie poziomu bezpieczeństwa i anonimowości, na jakich nam zależy. To ustawienie możemy zmienić później, jeśli zmienimy zdanie.



1 W celu zmiany ustawień bezpieczeństwa, po uruchomieniu przeglądarki na górnym pasku klikamy na symbol tarczy, a następnie na **Zmień** **A**.

2 Do wyboru mamy trzy ustawienia **B**, wystarczy wybrać poziom ochrony, który nas interesuje, zmiana nastąpi natychmiastowo.

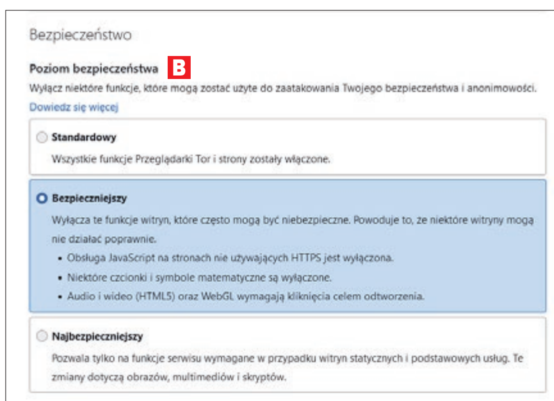
3 Teraz możemy rozpocząć korzystanie z przeglądarki.

TRZY POZIOMY BEZPIECZEŃSTWA DO WYBORU

1 **Standardowy** – jest to standardowy poziom przeznaczony dla użytkowników, którzy nie potrzebują ochrony i nie zależy im na zachowaniu maksymalnej anonimowości.

2 **Bezpieczniejszy** – ten poziom oferuje najbardziej optymalne ustawienia ochrony, które nie powinny w znaczący sposób wpłynąć na komfort korzystania z przeglądarki. Nie pozwala na uruchamianie skryptów na stronach bez protokołu HTTPS, nie pozwala na automatyczne wyświetlanie elementów audio i wideo bez zgody użytkownika i wielu innych. Zaleca się wypróbowanie tego poziomu od razu po zainstalowaniu przeglądarki.

3 **Najbezpieczniejszy** – oferuje ochronę na najwyższym poziomie. Skrypty wyłączone są na wszystkich typach stron, a dodatkowo mogą być blokowane na przykład pliki czcionek i obrazów. Dotyczy to również filmów i plików audio. Sprawia to, że korzystanie z przeglądarki w tym trybie jest wysoce niekomfortowe i czasami uciążliwe dla zwykłego użytkownika.



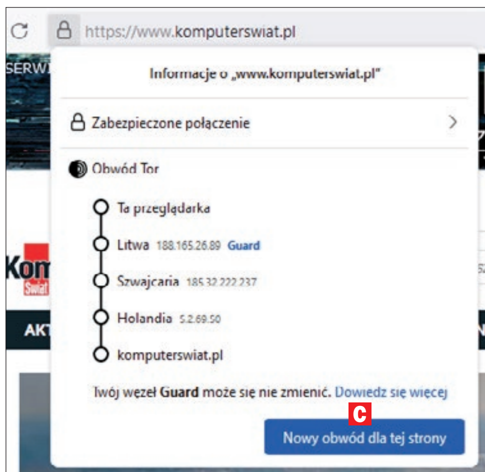
Obwód Tor a adres IP

Po wejściu na jakąkolwiek stronę internetową będziemy mogli sprawdzić nasz obwód Tor, czyli

adam13zajac@gmail.com

drogę poprzez poszczególne węzły sieci Tor – od wejściowego do wyjściowego. Na podanym przykładzie możemy zauważyć, że ruch kierowany jest przez trzy różne kraje i różne adresy IP. Naszym finalnym adresem jest adres węzła znajdującego się na samym dole, w tym przypadku **Holandia**. Adres początkowy nie ma tutaj znaczenia, gdyż każda strona, z którą będziemy się łączyli, będzie w stanie rozpoznać tylko i wyłącznie adres IP ostatniego węzła sieci Tor. Jest to szczególnie istotne, gdy na przykład jakieś treści w internecie nie są dostępne dla użytkowników z Polski lub Europy, ponieważ jeśli adres IP końcowego węzła będzie na przykład z USA, zostaniemy dopuszczeni do cenzurowanej treści.
W każdej chwili możemy zmienić tożsamość, czyli wybrać losowo nowe węzły dla całej przeglądarki lub wybrać nowy obwód tylko dla wybranej strony.

1 Klikamy na ikonę kłódki na górnym pasku nawigacyjnym przeglądarki.



2 Następnie wybieramy opcję **Nowy obwód dla tej strony** **C**.

3 Po wybraniu tej opcji zostaniemy przełączeni na inny węzeł, a strona zostanie załadowana ponownie.

Bezpieczne wiadomości e-mail

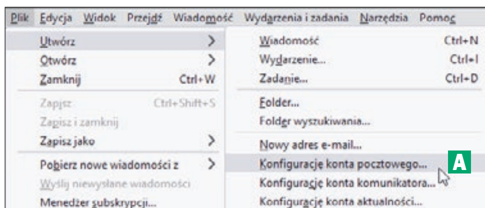
W rozdziale **2** poznaliśmy już program, który pozwala korzystać z bezpiecznej komunikacji e-mail. Przeczytajmy teraz, jak go w praktyce skonfigurować i zacząć korzystać z szyfrowania wiadomości na co dzień. Porady są oparte na programie **Mozilla Thunderbird** (**DVD-KOD: 053/054** 32-/64-BIT) – wszechstronnym i zarazem bezpiecznym.

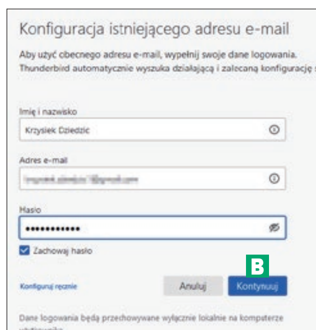
Dodajemy konto pocztowe

1 Instalujemy klienta poczty **Thunderbird**.

2 Uruchamiamy program i w głównym oknie klikamy na **Plik**, **Utwórz**, **Konfigurację konta pocztowego** **A**.

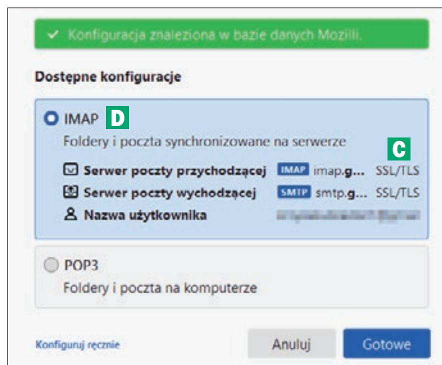
3 Teraz podajemy wymagane dane i klikamy na **Kontynuuj** **B**.





adam13zajac@gmail.com

4 Program powinien prawidłowo rozpoznać serwery e-mail naszego konta. Upewniamy się, czy przy obydwu pozycjach na końcu jest **SSL** lub **TLS** **C**, co oznacza wsparcie szyfrowania. Pozostawiamy zaznaczoną opcję **IMAP** **D** i klikamy na **Gotowe**.



5 Teraz możemy uzyskać dostęp do naszego konta dzięki Thunderbirdowi **F**.

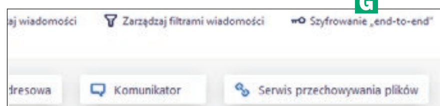
Korzystamy z szyfrowania typu end-to-end

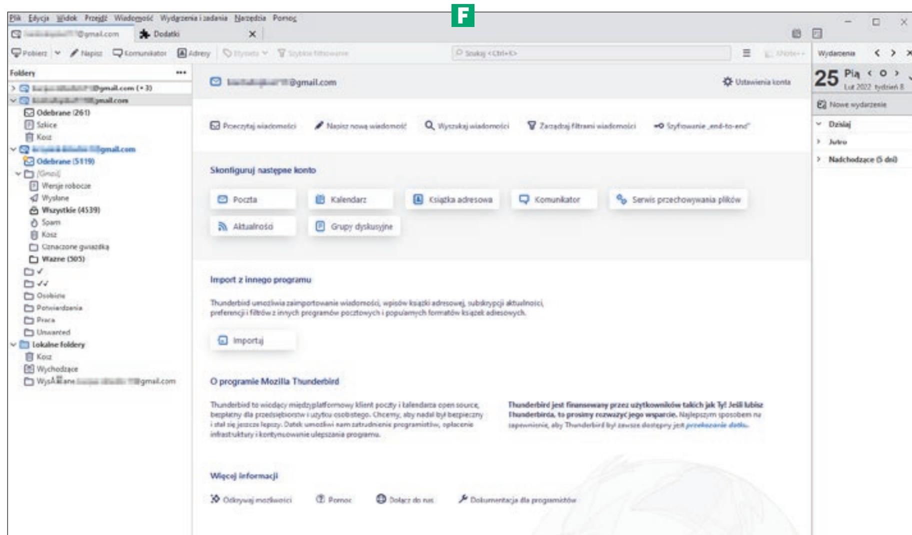
Thunderbird wspiera szyfrowanie wiadomości typu end-to-end, co oznacza, że wiadomość zaszyfrowana po naszej stronie zostanie odszyfrowana dopiero przez naszego odbiorcę i nikt po drodze nie będzie mógł poznać treści takiej wiadomości.

UWAGA!

Wszystkie e-maile przechowywane są na naszym dysku. Jeśli zależy nam na bezpieczeństwie, powinniśmy zadbać o zaszyfrowanie dysku lub chociaż wrażliwych lokalizacji, takich jak folder przechowujący naszą pocztę. Nawet jeśli stosujemy szyfrowanie podczas wysyłania i odbierania e-maili, osoby trzecie mogą uzyskać dostęp do wiadomości z naszego dysku.

1 Po podpięciu konta pocztowego możemy aktywować dla niego szyfrowanie typu end-to-end. W tym celu klikamy na główny folder naszego konta, a następnie po prawej stronie klikamy na **Szyfrowanie „end-to-end”** **G**.





adam13zajac@gmail.com

2 Teraz po prawej stronie klikamy na **Dodaj klucz** w polu **OpenPGP**.

ystanie z OpenPGP, lub certyfikat osobisty, aby umożliwić korzystanie
posiadasz odpowiedni tajny klucz. Więcej informacji

OpenPGP dla tożsamości

Dodaj klucz...

ać i zarządzać kluczami publicznymi swoich rozmówców oraz wszystkimi

3 Następnie wybieramy opcję **Utwórz nowy klucz OpenPGP** i klikamy na **Kontynuuj**.

Jeśli masz już klucz osobisty dla tego adresu e-mail, zaimportuj go. W przeciwnym razie nie będziesz mieć dostępu do swoich archiwów zaszyfrowanych wiadomości, ani nie będziesz w stanie odczytać przychodzących zaszyfrowanych wiadomości e-mail od osób, które nadal używają Twojego istniejącego klucza. Więcej informacji

Utwórz nowy klucz OpenPGP

Importuj istniejący klucz OpenPGP

Kontynuuj Anuluj

4 Ustalamy ważność klucza – na przykład **2 lata** **H** – oraz rozmiar klucza **4096** **I**, po czym klikamy na **Wygeneruj klucz**.

Ważność klucza

Określ czas wygaśnięcia nowo utworzonego klucza. Możesz później zmienić datę, aby w razie potrzeby przedłużyć ten czas.

Klucz wygasa za 2 lat(a) H

Klucz nie wygasa

Ustawienia zaawansowane

Zaawansowane ustawienia klucza OpenPGP.

Typ klucza: RSA

Rozmiar klucza: 4096 I

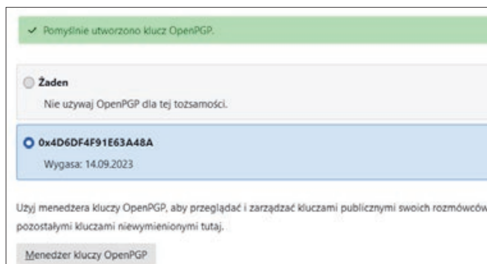
5 W kolejnym kroku klikamy na **Potwierdź** w celu rozpoczęcia generowania pary kluczy.

Generowanie klucza może zająć nawet kilka minut. Nie wyłączaj aplikacji w trakcie generowania. Aktywne przeglądanie Internetu i wykonywanie działań intensywnie korzystających z dysku podczas generowania klucza uzupełni „pulę losowości" i przyspieszy ten proces. Po ukończeniu generowania zostanie wyświetlony komunikat.

Wygenerować publiczny klucz i tajny klucz dla „[redacted]gmail.com"?

Anuluj Potwierdź

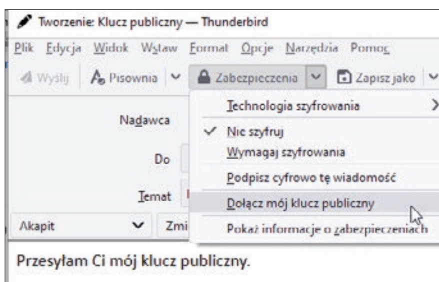
6 Po chwili para kluczy zostanie utworzona – tajny klucz jest tylko dla nas, publiczny możemy udostępniać znajomym.



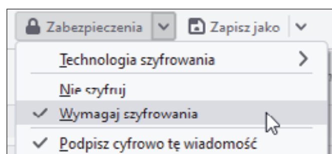
Wymieniamy się kluczami publicznymi

Należy wymienić się kluczami publicznymi z naszymi odbiorcami, tylko dzięki temu będziemy mogli później odszyfrować wiadomości – podobnie nasi odbiorcy.

1 W celu przesłania publicznego klucza rozpoczynamy tworzenie wiadomości e-mail, a potem na pasku górnym z zakładki **Zabezpieczenia** wybieramy opcję **Dołącz mój klucz publiczny**.



2 Odbiorca musi następnie kliknąć prawym przyciskiem myszy na załączony klucz publiczny i wybrać opcję **Importuj klucz OpenPGP**. Dopiero wtedy będziemy mogli w zakładce **Zabezpieczenia** wybrać opcję **Wymagaj szyfrowania** oraz **Podpisz cyfrowo tę wiadomość**. Musimy jedynie być pewni, że zarówno my, jak i nasz odbiorca mamy klucze publiczne. W innym wypadku nie będziemy mogli odszyfrować wiadomości.



adam13zajac@gmail.com

CO TO JEST VPN

Jest to nic innego jak **Wirtualna Sieć Prywatna** (ang. **Virtual Private Network**). Popularnie połączenia w takiej sieci nazywa się tunelowanymi, ponieważ transmisja pakietów jest zaszyfrowana pomiędzy dwoma punktami, które w ten sposób tworzą „tunel” w internecie. Takie rozwiązania sieciowe są szeroko wykorzystywane w firmach, ponieważ zapewniają wysoki poziom bezpieczeństwa przy niskich kosztach. Pracownik może uzyskać dostęp do zasobów w firmie w każdej chwili, a przy tym nikt nie będzie mógł zweryfikować, jakie dane są przesyłane. Dla domowego użytkownika korzystanie z sieci VPN jest również bardzo atrakcyjne, gdyż pozwala w bardzo bezpieczny i na pewien sposób anonimowy uzyskać dostęp do zasobów internetu. Możemy z takiego typu połączenia korzystać praktycznie w każdej chwili i jest niezwykle przydatne, na przykład gdy jesteśmy zmuszeni do korzystania z otwartych sieci lub publicznych – hotspotów. Przy normalnym połączeniu administrator sieci i dostawca internetu mają wgląd w nasze pakiety. Jednak jeśli skorzystamy z możliwości połączeń z siecią VPN, ruch, który będziemy generować, zostanie zaszyfrowany i będziemy mogli na przykład skorzystać z bankowości internetowej w bezpieczny sposób.
Warto wypróbować programy VPN, które znajdziemy na płycie dołączonej do książki – **OpenVPN** (DVD-KOD: 032/033 32-/64-BIT), **ProtonVPN** (DVD-KOD: 035) oraz **Windscribe VPN** (DVD-KOD: 061). Korzystanie z tego ostatniego zostało opisane na stronach 13 i 14, a w tym rozdziale skupimy się na OpenVPN.

Korzystamy z OpenVPN w Windows

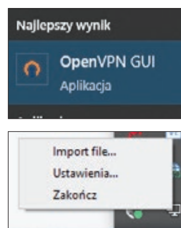
Jeśli zależy nam na bezpieczeństwie i anonimowości, to najlepszym wyborem jest skorzystanie z protokołu OpenVPN. Przeczytajmy, jak korzystać z niego w systemie Windows.

1 Zaczynamy od instalacji klienta OpenVPN na naszym urządzeniu. **Uwaga!** Nie zmieniajmy żadnych domyślnych ustawień.

2 Musimy również wyrazić zgodę na instalację specjalnego sterownika wirtualnej sieci, bez którego nie będzie możliwe łączenie się z serwerami.
Warto wiedzieć: Po uruchomieniu programu nie będziemy mogli od razu skorzystać z możliwości bezpiecznego połączenia, musimy dograć pliki konfiguracyjne, które na to pozwolą.

3 Uruchamiamy **OpenVPN GUI**.

4 Następnie klikamy prawym przyciskiem myszy na ikonę w zasobniku systemowym, a później na **Ustawienia**.



5 Przechodzimy do zakładki **Advanced** A i sprawdzamy lokalizację folderu, w którym powinny być pliki konfiguracyjne – pole **Configuration Files** B. Otwieramy Eksplorator i nawigujemy do tej lokalizacji.

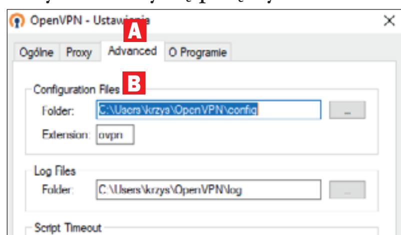
6 Teraz za pomocą przeglądarki wchodzimy na adres **vpngate.net/en**, możemy również skorzystać z innych stron oferujących darmowy lub płatny dostęp do ser-

adam13zajac@gmail.com

Do you want to parse the below HTML table? Instead you can use CSV List to make your own VPN Gate client app.

Country (Physical location)	DDNS hostname IP Address (ISP hostname)	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative transfers Logging policy	SSL-VPN Windows (comfortable)	L2TP/IPsec Windows, Mac, iPhone, Android No client required	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT No client required
Japan	public-vpn-97.opengw.net 219.100.37.83 (public-vpn-06-03.vpngate.v4.open.ad.jp)	95 sessions 19 days Total 4,671,001 users	1,541.35 Mbps Ping: 31 ms 198,685.22 GB Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443	MS-SSTP Connect guide SSTP Hostname : public-vpn-97.opengw.net
Japan	public-vpn-206.opengw.net 219.100.37.165 (public-vpn-11-05.vpngate.v4.open.ad.jp)	78 sessions 19 days Total 4,817,994 users	378.17 Mbps Ping: 18 ms 166,872.61 GB Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443 **C**	MS-SSTP Connect guide SSTP Hostname : public-vpn-206.opengw.net

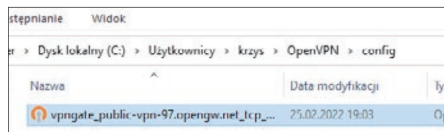
werów VPN. Na podanej stronie klikamy na **OpenVPN Config file** **C** przy serwerze, z którym chcemy się połączyć.

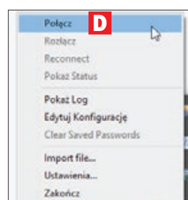


7 Następnie klikamy na link w celu pobrania pliku z konfiguracją.



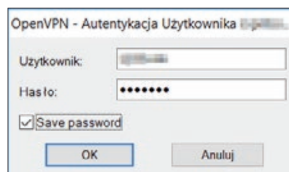
8 Przenosimy pobrany plik z rozszerzeniem **OVPN** do folderu przeznaczonego na pliki konfiguracyjne.





9 Teraz zamykamy i ponownie uruchamiamy klienta OpenVPN. Po kliknięciu prawym przyciskiem myszy na ikonę klienta zobaczymy opcję **Połącz** **D** – wystarczy na nią kliknąć.

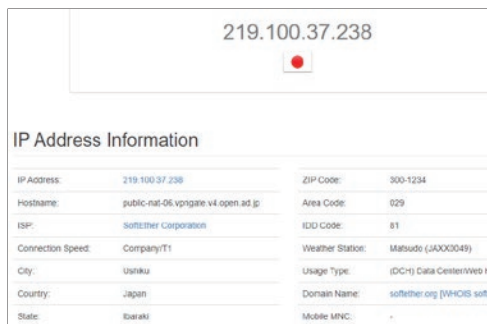
10 W zależności od wybranego serwera może pojawić się okno z prośbą o podanie loginu i hasła, dla serwerów na powyższej stronie te dane to **vpn** i **vpn**. Zaznaczamy opcję **Save password** i klikamy na **OK**.



11 Po poprawnym zestawieniu połączenia ikona klienta OpenVPN zmieni wygląd na zielony monitor.



12 Gdy sprawdzimy nasz adres IP po zestawieniu połączenia, okaże się, że łączymy się szyfrowanym połączeniem z serwerem w Japonii.

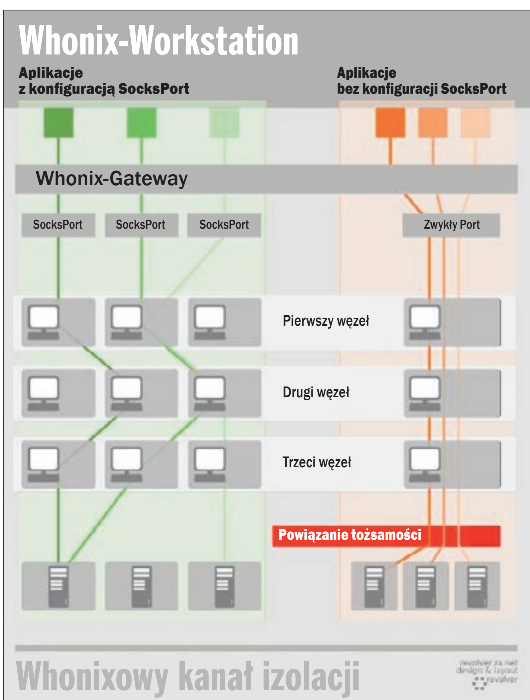


adam13zajac@gmail.com

6 System, który zapewnia prywatność i anonimowość – Whonix

Jeśli zależy nam na tym, aby być w sieci całkowicie anonimowym i na każdym kroku dbać o swoją prywatność i bezpieczeństwo danych – warto skorzystać z systemu Whonix, który może nam to zapewnić. W tym rozdziale przeczytamy, jak krok po kroku z niego korzystać

Whonix (DVD-KOD: 060) to sprawdzony system operacyjny dla osób, które chcą zachować anonimowość i prywatność w sieci. Jest to jedno z najlepszych rozwiązań dla użytkowników prywatnych, które nie wymaga ogromnej wiedzy i jest dość łatwe w obsłudze. Whonix wykorzystuje oprogramowanie VirtualBox do wirtualizacji i jest oparty na dystrybucji Debian. Najważniejszą funkcją tego systemu jest to, że każde połączenie sieciowe zostanie automatycznie zanonimizowane poprzez wykorzystanie bezpiecznej sieci Tor. Dzięki temu mamy pewność, że żadne informacje dotyczące nas, w tym adres IP oraz lokalizacja, nie zostaną zdradzone.



Tor SocksPort

Dzięki mechanizmowi Tor SocksPort, z którego korzysta wiele aplikacji w systemie Whonix, odkrycie prawdziwej tożsamości użytkownika

adam13zajac@gmail.com

JAK TO DZIAŁA



Czerwone strzałki wskazują na to, że niezabezpieczone aplikacje nie mogą wydostać się poza maszynę Whonix-Workstation

Wszystkie połączenia sieciowe są przepuszczane przez maszynę Whonix-Gateway, gdzie są przerzucane na sieć Tor i dopiero uzyskają dostęp do internetu

Whonix do działania wymaga dwóch wirtualnych maszyn pracujących jednocześnie w systemie użytkownika – są to **Whonix-Gateway** oraz **Whonix-Workstation**.
Ta pierwsza działa na zasadzie bramy i obsługuje wszelkie procesy sieci Tor. Druga natomiast pozwala na korzystanie z aplikacji w całkowicie wyizolowanym środowisku i uzyskuje dostęp do sieci poprzez maszynę **Whonix-Gateway**.
Takie rozwiązanie pozwala na uzyskanie wielu korzyści dla użytkownika:

- Tylko połączenia z siecią Tor są dozwolone
- Serwery oraz aplikacje mogą nawiązywać jedynie bezpieczne połączenia
- Wycieki danych przez DNS są niemożliwe
- Szkodliwe programy nawet z uprawnieniami administratora nie są w stanie odkryć prawdziwego adresu IP użytkownika
- Niebezpieczeństwo wycieku danych z aplikacji lub serwerów jest zminimalizowane

jest dodatkowo utrudnione, ponieważ ruch aplikacji, takich jak Thunderbird, Tor Browser, Hexchat, jest kierowany przez różne obwody sieci Tor i dzięki temu powiązanie danych jednego użytkownika jest dodatkowo utrudnione.

Uruchamiamy Whonix

Do korzystania z systemu Whonix konieczne jest zainstalowanie programu **VirtualBox** (DVD-KOD: 059), który jest dostępny na płycie.

Gdy nie mamy zainstalowanego programu VirtualBox

1 Uruchamiamy instalator programu VirtualBox, klikamy na **Next** i przechodzimy przez kolejne kroki kreatora.



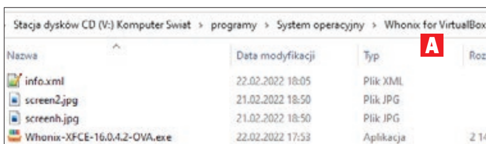
adam13zajac@gmail.com

2 Po poprawnej instalacji wszystkich sterowników i samego programu możemy przejść do wykonywania kolejnych wskazówek.

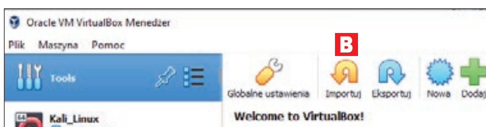


Gdy mamy już zainstalowany program VirtualBox

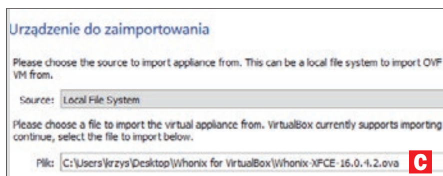
W tym przypadku możemy od razu przejść do importowania maszyn wirtualnych do programu VirtualBox. Znajdziemy je w folderze **Whonix for VirtualBox** **A** na płycie dołączonej do książki. Są one spakowane w samowypakowujące się archiwum.



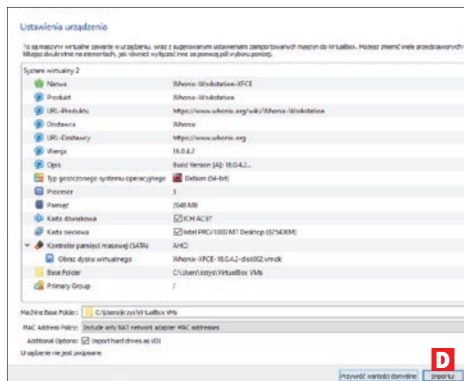
1 Uruchamiamy VirtualBox i klikamy na **Importuj** **B**.



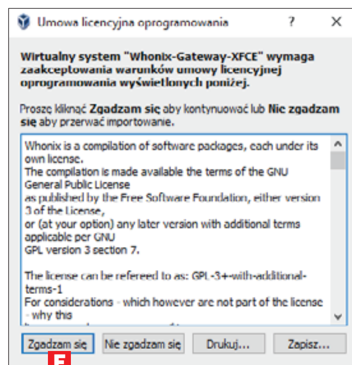
2 Następnie wskazujemy wypakowany plik **C** na naszym dysku i klikamy na **Dalej**.



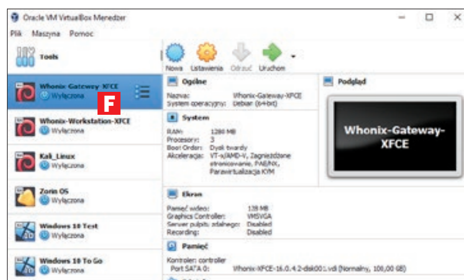
3 Pojawią się dane maszyn, jakie zostaną zaimportowane – w tym przypadku będą to **Whonix-Gateway** oraz **Whonix-Workstation**. Wszelkie ustawienia pozostawiamy bez zmian i klikamy na **Importuj** **D**.



4 W kolejnym kroku wyrażamy zgodę na licencję, klikając na **Zgadzam się** **E**.



5 Po dłuższej chwili maszyny będą widoczne w oknie programu VirtualBox **F**.



adam13zajac@gmail.com

DOMYŚLNE DANE LOGOWANIA ADMINISTRATORA

Jeśli po raz pierwszy korzystamy z systemu Whonix, domyślne dane logowania to **Użytkownik: user**, a **Hasło: changeme**. Po zalogowaniu do systemu możemy zmienić hasło. Należy uruchomić Terminal, klikając na jego ikonę w górnym lewym rogu ekranu, a następnie wpisać polecenie **passwd** i podać stare hasło, a następnie nowe hasło.

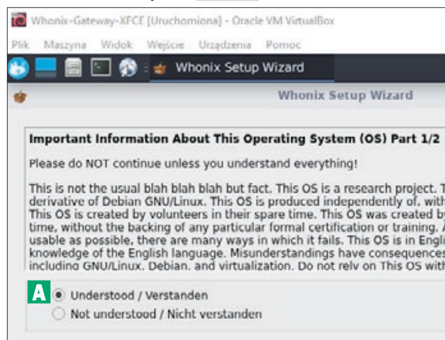
```
Type: "whonix" <enter> for help.
user@host:~$ passwd
Changing password for user.
Current password:
New password:
Retype new password:
passwd: password updated successfully
user@host:~$
```

6 Następnie uruchamiamy maszynę Whonix-Gateway i od razu po niej Whonix-Workstation i przechodzimy do korzystania z systemu.

Uwaga! Zawsze uruchamiamy Whonix-Gateway jako pierwszą maszynę i dopiero, gdy poprawnie się uruchomi, przystępujemy do uruchomienia Whonix-Workstation.

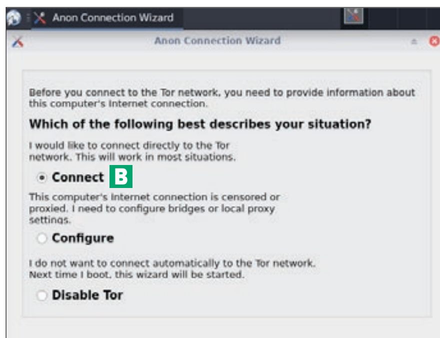
Pierwsze kroki z Whonix

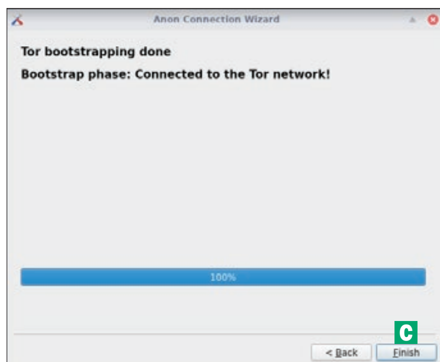
1 Po uruchomieniu maszyn musimy na każdej z osobna zaznaczyć dwukrotnie opcję **Understand** **A** i kliknąć na **Next**. Na koniec klikamy na **Finish**.



2 Następnie na maszynie **Whonix-Gateway** zostanie uruchomiony program **Anon Connection Wizard**. Zaznaczamy w nim opcję **Connect** **B** i klikamy na **Next**.

3 W kolejnym kroku zostanie podjęta próba nawiązania połączenia z siecią Tor. Jeśli się powiedzie, pojawi się komunikat o sukcesie. Klikamy na **Finish** **C**.





4 Dopiero od tej chwili w maszynie **Whonix-Workstation** zostanie nawiązane połączenie sieciowe i rozpocznie się proces sprawdzania aktualizacji oraz samego połączenia.

5 Po chwili powinniśmy mieć dostęp do internetu na każdej z wirtualnych maszyn.

6 W każdej z nich musimy przeprowadzić aktualizację. Klikamy na górnym pasku po lewej stronie na ikonę Terminalu **D**.

7 Następnie wpisujemy polecenie **sudo apt-get-update-plus dist-upgrade** **E** i wciskamy klawisz enter.

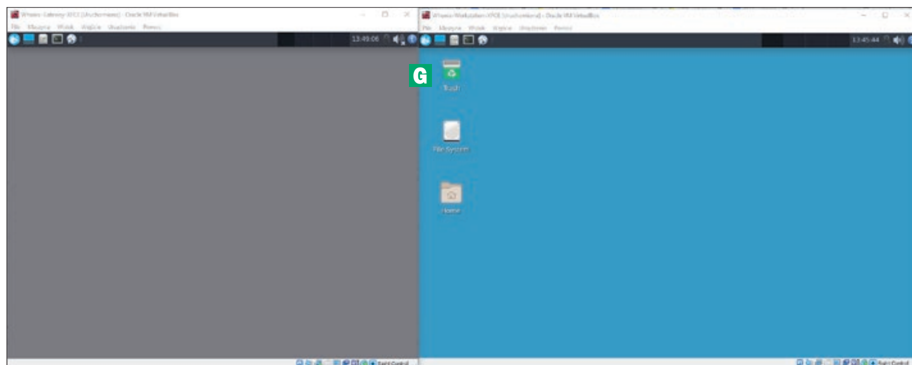
```
default user account: user
default password: changeme

Type: "whonix" <enter> for help.
user@host:~$ sudo apt-get-update-plus dist-upgrade
Hit:1 tor+https://deb.debian.org/debian bullseye In
```

8 Po chwili należy wpisać w Terminalu **Y** **F** i ponownie zatwierdzić klawiszem enter wykonanie instalacji.

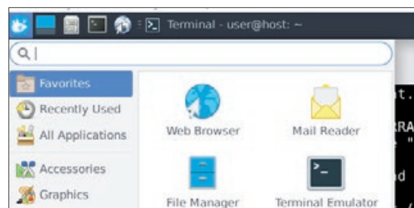
```
The following packages will be upgraded:
  libexpat1 libjavascriptcoregtk-4.0-18 libwebkit2gtk-4.0-37
3 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 20.5 MB of archives.
After this operation, 222 kB of additional disk space will be used
Do you want to continue? [Y/n]
```

9 Po zakończeniu całego procesu należy ponownie uruchomić obydwie maszyny wirtualne **G**.



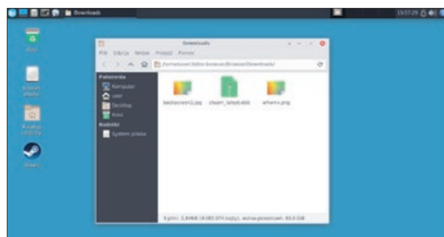
Korzystamy z Whonix

Bardzo ważne jest, aby pamiętać, że od tej pory z maszyny **Whonix-Gateway** nie należy korzystać w celu normalnej pracy, ale musi ona być aktywna w tle, ponieważ zapewnia ruch sieciowy naszej głównej maszynie. Wszelkie programy, aplikacje uruchamiamy tylko i wyłącznie na maszynie **Whonix-Workstation**.
Obsługa systemu jest dość prosta. Gdy dojdziemy do tego etapu, nasze połączenie sieciowe jest bezpieczne i nie musimy się martwić wyciekami danych. Na górze ekranu znajduje się pasek zadań. Po lewej stronie po kliknięciu na ikonę menu Start pojawi się menu z wszystkimi aplikacjami i paskiem wyszukiwania.



adam13zajac@gmail.com

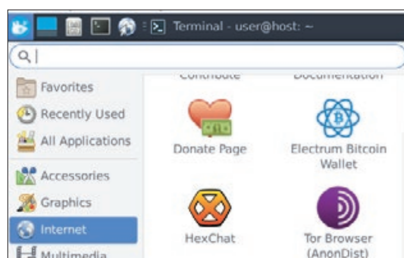
Standardowo Whonix uruchamiany jest w trybie **Persistent**. Oznacza to, że wszystkie zapisane pliki w trakcie korzystania z systemu, aktualizacje i pobrane elementy zostają zapisane na maszynie wirtualnej – tak jakby miało to miejsce w normalnym systemie operacyjnym. Możemy więc bez problemu zachowywać różnego typu dane – nie zostaną one usunięte przy ponownym uruchomieniu maszyny.



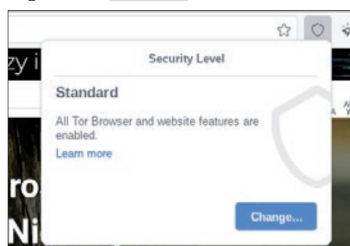
Anonimowość w przeglądarce

Domyślna przeglądarka Whonix to Tor Browser. Przed pierwszym użyciem musimy ustalić, jaki poziom bezpieczeństwa nas interesuje.

1 Klikamy na menu Start, następnie na kategorię **Internet**, a potem na **Tor Browser**.



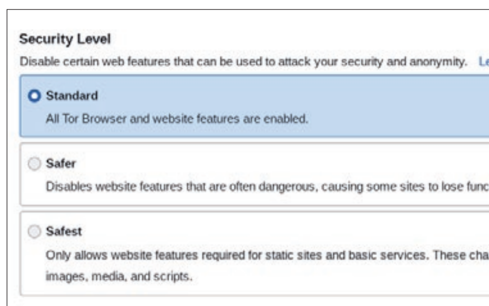
2 Po uruchomieniu przeglądarki klikamy na pasku adresowym na symbol tarczy, a następnie na **Change**.



BANKI I PŁATNOŚCI

Obecnie jeśli chcemy w pełni korzystać ze wszystkich witryn, i tak musimy poświęcić swoją anonimowość, na przykład podczas logowania się do banku czy też dokonywania zakupów i płacenia przez internet. W przypadku takich operacji najlepiej nie korzystać z Whonix i innych anonimowych rozwiązań, gdyż logowanie do banku może zostać zablokowane, a transakcje odrzucone ze względu na nieznany adres IP z wewnątrz sieci Tor.

3 Teraz wybieramy poziom ochrony, jaki nam odpowiada – jeśli zależy nam na najwyższym poziomie bezpieczeństwa, należy wybrać opcję **Safest**. **Uwaga!** Po wybraniu tej opcji część stron internetowych może nie działać prawidłowo.



4 Od tej chwili możemy bezpiecznie i anonimowo przeglądać zasoby internetu.

Instalacja aplikacji niedostępnych w standardowych repozytoriach

W repozytoriach dostępnych dla Whonix znajdziemy tylko i wyłącznie sprawdzone i przetestowane oprogramowanie dostępne na zasadach licencji open source. W przypadku próby zainstalowania programów takich jak Steam, Skype, Chrome, które nie należą do wolnego oprogramowania, będziemy musieli postępować według zupełnie innej procedury. Poznajmy ją na przykładzie programu **Steam**.

adam13zajac@gmail.com

INSTALACJA DODATKOWYCH APLIKACJI

Jeśli chcemy zachować anonimowość na najwyższym poziomie, najlepiej nie instalować dodatkowych aplikacji. Na przykład instalując przeglądarkę Google Chrome, a następnie logując się na nasze konto, pomimo korzystania z sieci Tor tracimy anonimowość. Niezależnie od tego, jakim adresem IP się identyfikujemy, można rozpoznać nas po identyfikatorze użytkownika. W przypadku gdy instalacja konkretnej aplikacji jest dla nas niezbędna, w każdej chwili możemy jej dokonać. Procedura jest nieco bardziej skomplikowana niż w nowocześniejszych systemach Linux i wymaga obsługi Terminalu. Dla przykładu zainstalujemy program GIMP do edycji grafiki.

1 Uruchamiamy Terminal, wpisujemy polecenie **sudo apt-get install gimp**, zatwierdzamy klawiszem enter i podajemy hasło administratora.

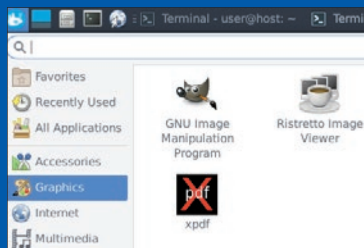
```
Type: "whonix" <enter> for help.
user@host:~$ sudo apt-get install gimp
[sudo] password for user:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

2 Potwierdzamy pobieranie plików i instalację, wpisując **Y** i zatwierdzając klawiszem enter.

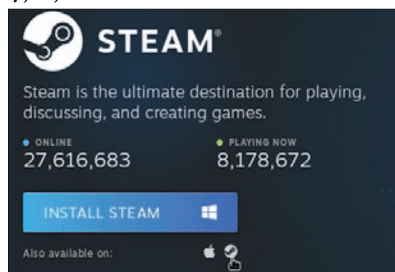
```
  libwmf0.2-7 poppler-data
0 upgraded, 51 newly installed, 0 to remove and 0 not upgraded.
Need to get 57.5 MB of archives.
After this operation, 232 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

3 Po zakończeniu instalacji naszą aplikację znajdziemy w menu startowym w odpowiedniej kategorii, w tym przypadku **Graphics**.

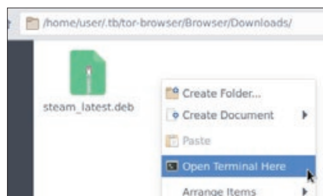
Można sprawdzić, jak instalować dodatkowe aplikacje dla systemu Whonix, wyszukując je w internecie – należy szukać instrukcji przewidzianych dla systemu Debian.



1 Na początku musimy pobrać paczkę instalacyjną ze strony twórcy. W tym przypadku przechodzimy na stronę **store.steampowered.com/about** i klikamy na ikonę Steam w celu pobrania paczki instalacyjnej. Musi ona mieć rozszerzenie **DEB**.



2 Uruchamiamy **Menedżer plików**, przechodzimy do lokalizacji z pobraną paczką, klikamy prawym przyciskiem myszy na wolną przestrzeń i z menu kontekstowego wybieramy opcję **Open Terminal Here**.



3 Wpisujemy komendę **sudo su**, następnie **sudo apt install ./steam_latest.deb** Każdą zatwierdzamy i podajemy hasło.

adam13zajac@gmail.com

4 Zatwierdzamy instalację, wpisując **Y** i zatwierdzając klawiszem enter.

```
The following NEW packages will be installed:
  python-apt-common python3-apt steam-launcher
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 286 kB/3,872 kB of archives.
After this operation, 5,069 kB of additional disk space will be
Do you want to continue? [Y/n]
```

5 Po chwili w menu Start w kategorii **Games** pojawi się aplikacja **Steam**.

6 Proces instalacji dodatkowych aplikacji spoza repozytorium sprowadza się więc do pobrania paczki instalacyjnej z rozszerzeniem **DEB**, a następnie instalacji tej paczki w Terminalu, wykorzystując odpowiednie komendy.

Zmiana języka na polski

Jeśli chcemy, możemy zmienić domyślny język systemu Whonix. Nie jest to tak proste jak w przypadku innych dystrybucji, i wymaga skorzystania z Terminalu.

1 Uruchamiamy Terminal, wpisujemy i zatwierdzamy polecenie **sudo dpkg-reconfigure locales**

```
user@host:~$ sudo dpkg-reconfigure locales
```

2 Następnie wybieramy z listy opcję **pl_PL.UTF-8 UTF-8**, a usuwamy zaznaczenie z opcji **en_US.UTF-8**. Modyfikacji dokonujemy, wciskając klawisz spacja, a na koniec wciskamy klawisz enter.

USUWAMY ZBĘDNY WPIS W TERMINALU

Domyślnie przy każdym uruchomieniu programu Terminal pojawia się długa informacja wstępna, która zajmuje cały ekran. Można dość prosto się jej pozbyć. Uruchamiamy Terminal i wpisujemy komendę **cp /etc/skel/.bashrc.whonix-orig ~/.bashrc**

```
Whonix is a research project.

default user account: user
default password: changeme

Type: "whonix" <enter> for help.
user@host:~$ cp /etc/skel/.bashrc.whonix-orig ~/.bashrc
user@host:~$
```

Po ponownym uruchomieniu Terminalu będziemy mogli już korzystać z niego bez wstępnej informacji oraz z kolorowymi filtrami.

3 W kolejnym oknie wybieramy dodaną przed chwilą polską opcję językową i wciskamy klawisz enter.

4 Po chwili zostaną wygenerowane pliki locale i będziemy mogli ponownie uruchomić wirtualną maszynę.

5 Po ponownym uruchomieniu system będzie działał już w polskiej wersji językowej.

adam13zajac@gmail.com

7 Prywatność na smartfonie

Z poprzednich rozdziałów dowiedzieliśmy się wiele na temat zachowania prywatności na komputerze. Warto również nauczyć się tego samego w wypadku smartfona, który coraz częściej zastępuje nam komputer. Coraz częściej też staje się obiektem ataków mających na celu zdobycie naszych danych

Prywatność, anonimowość i smartfon

Zupełne zniknięcie ze świata i jednocześnie korzystanie ze smartfona jest praktycznie niemożliwe.

Ciągły postęp technologiczny daje zupełnie nowe metody inwigilacji, a jednocześnie – ochrony przed nią. Nieustanna walka pomiędzy tymi, którzy chcą podsłuchiwać rozmowy i śledzić działania wykonywane na smartfonach, a tymi, którzy chcą zupełnie „zniknąć z radarów", sprawia, że zwykli użytkownicy muszą coraz bardziej uważać, wykonując codzienne czynności.

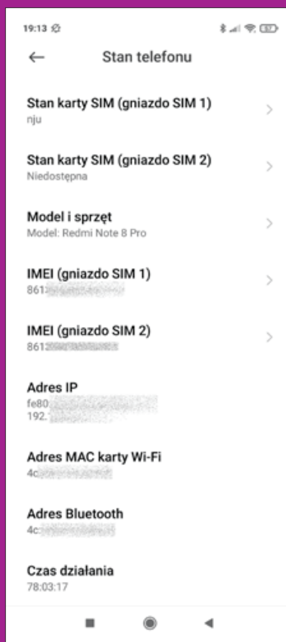
Smartfony dają ogromne możliwości – możemy przeglądać internet, rozmawiać z bliskimi, wysyłać wiadomości tekstowe, multimedialne, prowadzić wideorozmowy, wykonywać płatności, korzystać z bankowości mobilnej, nawigować do wybranych miejsc i wiele więcej. Każda z tych czynności wymaga użycia aplikacji, a jej twórcy mogą zbierać mnóstwo informacji na nasz temat, na przykład o naszych zainteresowaniach, o tym, jakich informacji najczęściej szukamy czy dokąd podróżujemy.

Zarówno w wypadku urządzeń z systemem Android, jak i tych z iOS, mamy do dyspozycji kilka sposobów, by chronić naszą prywatność i móc zachować anonimowość.

adam13zajac@gmail.com

CAŁKOWITA ANONIMOWOŚĆ UŻYTKOWNIKA SMARTFONA – TO MOŻLIWE?

Jeśli zależy nam na całkowitej anonimowości, to w pełni legalnie nie da się jej osiągnąć, używając smartfona.
Obecnie w Polsce każdy numer telefonu musi zostać zarejestrowany i przypisany do konkretnej osoby.
Dodatkowo każdy smartfon ma indywidualny numer IMEI, który składa się z 15 cyfr i służy do identyfikacji urządzenia.
Taki numer możemy znaleźć w ustawieniach smartfona czy też w jego dokumentach lub wewnątrz obudowy.
Każdy operator na polecenie policji powinien udostępnić dane dotyczące działań wykonywanych przez konkretne urządzenie znajdujące się w sieci i podać przybliżoną lokalizację danego urządzenia.



Numer IMEI znajdziemy, wchodząc w **Ustawienia**, a następnie przechodząc do **O telefonie**, **Wszystkie parametry**, **Stan telefonu**

Jeżeli więc naprawdę chcemy być anonimowi, to przede wszystkim powinniśmy wyjąć kartę SIM, gdy chcemy się komunikować przez internet, i korzystać z sieci Wi-Fi, zachowując środki bezpieczeństwa opisane w tej książce.
Warto jednak zdawać sobie sprawę z tego, że oszuści mogą korzystać z nielegalnie zdobytych, na przykład za granicą, kart SIM zarejestrowanych na zupełnie inne osoby.
Takich kart nie można powiązać z ich faktycznymi użytkownikami, ale z numerem IMEI smartfona już tak.
Oczywiście i na to istnieją sposoby, chociaż nielegalne w Unii Europejskiej. Są smartfony, które mają wbudowane funkcje umożliwiające zmianę numeru IMEI na żądanie.

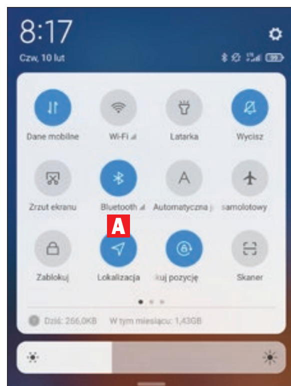
Śledzenie smartfona

Śledzenie urządzenia mobilnego, jakim jest smartfon, który praktycznie każdy nosi non stop przy sobie, może dostarczyć bardzo wielu informacji. Każdy smartfon ma wbudowany moduł GPS, który po aktywowaniu jest w stanie wskazać naszą aktualną pozycję geograficzną z dokładnością do 1–2 metrów. Warto wiedzieć, jak się chronić przed śledzeniem, na czym ono polega i jak wygląda oraz na co pozwala prawo.

Przede wszystkim śledzenie urządzenia, którego nie jesteśmy właścicielami, jest nielegalne. Za taki czyn grozi kara pozbawienia wolności do trzech lat. Ale jeśli chcemy na przykład śledzić smartfon naszego dziecka i jesteśmy właścicielami urządzenia, z którego korzysta, mamy do tego prawo.
Dodatkowo warto również wiedzieć, że operator na polecenie policji lub innych służb może podać przybliżoną lokalizację naszego

adam13zajac@gmail.com

urządzenia na podstawie numeru IMEI, o ile urządzenie pozostaje włączone. Co ciekawe, nie musi mieć ono aktywnej funkcji GPS. Operator jest w stanie wskazać obszar, na jakim urządzenie może się znajdować, na podstawie stacji bazowych. W dużych miastach, gdzie zagęszczenie takich stacji jest większe, lokalizacja będzie dokładniejsza niż na terenach podmiejskich, gdzie stacji jest mniej. Operator może zdalnie zablokować urządzenie, znając jedynie jego numer IMEI i nasz numer telefonu (warto więc na wszelki wypadek zapisać sobie IMEI – gdyby telefon został skradziony, mając IMEI, można wnioskować o jego zablokowanie).



Gdzie jest dziecko – śledzenie smartfona za pomocą Map Google

Większość operatorów daje możliwość kontroli własnego dziecka przez funkcję śledzenia w czasie rzeczywistym. Rodzic może skonfigurować odpowiednią aplikację na przykład w taki sposób, aby system automatycznie wysyłał SMS-y, gdy dziecko znajdzie się poza wyznaczonym obszarem. W zależności od operatora korzystanie z takiej funkcji może być płatne. Przeczytajmy, jak samemu, korzystając z darmowej aplikacji Mapy Google, skonfigurować śledzenie urządzenia naszej pociechy – bez dodatkowych opłat. Użyjemy funkcji udostępniania lokalizacji w Mapach Google.

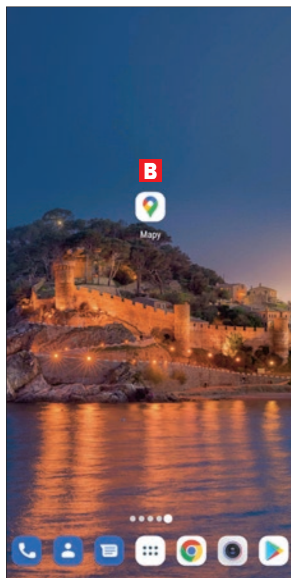
1 Do poprawnego działania udostępniania lokalizacji konieczne jest włączenie funkcji **GPS** oraz **danych mobilnych** w naszym urządzeniu. W większości smartfonów aktywujemy te funkcje, wyciągając górny pasek – **Szybkie ustawienia**. Funkcja GPS w części urządzeń może mieć nazwę **Lokalizacja** **A**.

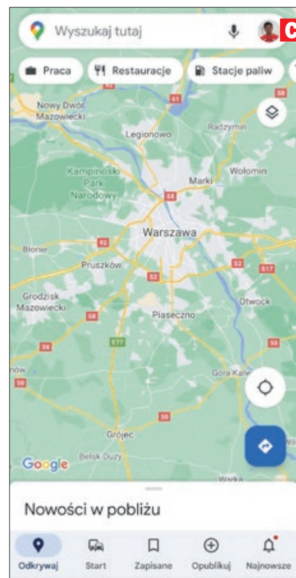
2 Następnie uruchamiamy aplikację **Mapy Google** **B** – jeśli jej nie mamy, instalujemy ją, korzystając ze sklepu Google Play.

3 Teraz musimy upewnić się, że jesteśmy zalogowani na nasze konto Google na urządzeniu, z którego chcemy śledzić pozycję dziecka; na urządzeniu dziecka powinniśmy być zalogowani innym kontem Google.

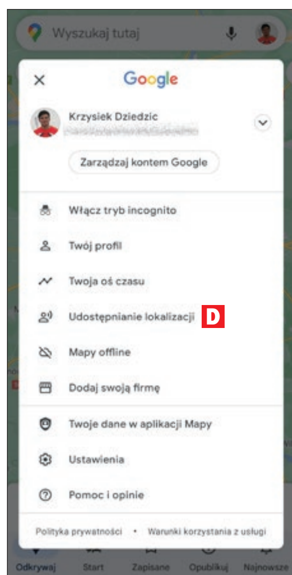
4 Następnie na urządzeniu dziecka klikamy w prawym górnym rogu na awatar konta **C**. Potem klikamy na **Udostępnianie lokalizacji** **D** i na **Nowe udostępnienie** **E**.

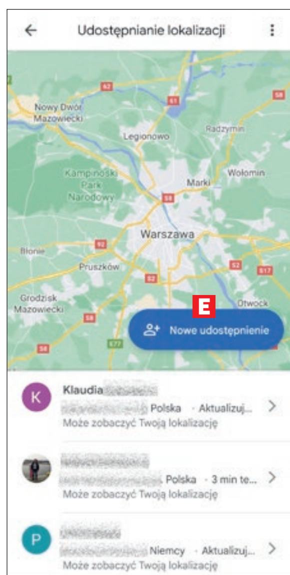
5 Jeśli zamierzamy korzystać ze śledzenia cały czas, wybieramy opcję **Dopóki nie wyłączę** **F**, a następnie wybieramy z listy osobę, której chcemy udostępniać lokalizację, czyli w naszym przykładzie – siebie.

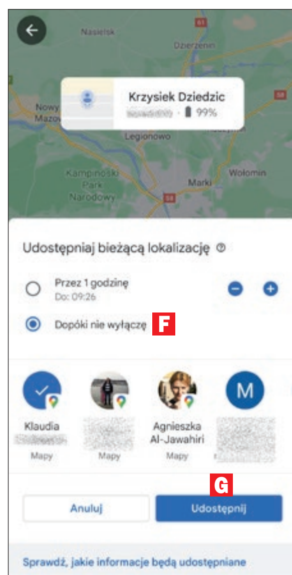




adam13zajac@gmail.com

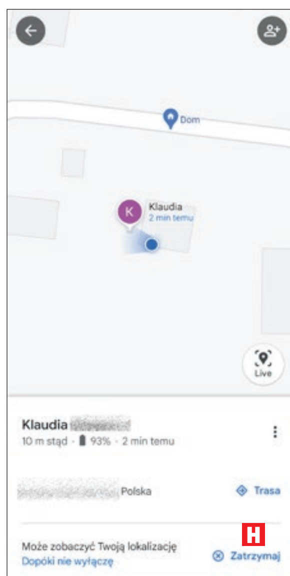






Można też wysłać informację o udostępnianiu poprzez SMS, e-mail lub inny komunikator. Klikamy na koniec na **Udostępnij** **G**.

6 Od tej chwili co kilka minut lokalizacja będzie aktualizowana i użytkownik, któremu udostępniliśmy te dane (czyli w naszym przykładzie my), będzie mógł znaleźć na mapie osobę, której lokalizacja została udostępniona (w naszym przykładzie dziecko), klikając na jej awatar lub wchodząc w **Udostępnianie lokalizacji** i wybierając ją z listy.



7 W każdej chwili można zatrzymać udostępnianie lokalizacji, klikając na **Zatrzymaj** **H** w ustawieniach udostępniania dla konkretnego użytkownika.

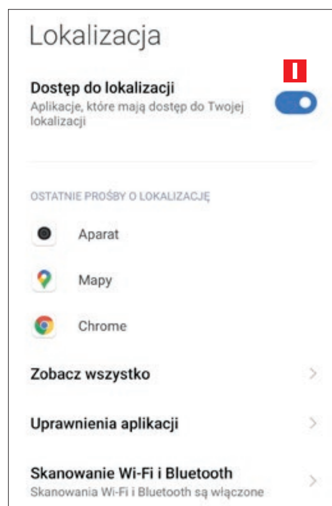
Warto pamiętać: Z opisanej funkcji w Mapach Google można oczywiście korzystać nie tylko w wypadku dziecka. Możemy w ten sposób udostępnić naszą lokalizację na przykład znajomym, z którymi mamy się spotkać, żeby wiedzieli, kiedy do nich dotrzemy albo gdzie nas szukać. Dostęp do lokalizacji wymaga zgody użytkownika danego konta Google.

Jak uniemożliwić śledzenie telefonu?

Najbardziej podstawowym krokiem w celu zablokowania śledzenia jest po prostu **wyłączenie funkcji GPS** (**Lokalizacja**) i korzystanie z tej opcji tylko i wyłącznie wtedy, gdy jest nam potrzebna podczas korzystania z nawigacji, na przykład z Map Google. Opcję GPS możemy wyłączyć w **Ustawieniach** naszego urządzenia – przechodzimy do **Lokalizacja** i wyłączamy opcję **Dostęp do lokalizacji** **I**. Oprócz tego możemy być również namierzani przez Wi-Fi – dokładność śledzenia

adam13zajac@gmail.com

poprzez Wi-Fi jest bardzo duża, gdyż sieci bezprzewodowe mają dość nieduży zasięg. Dlatego też należy **wyłączać Wi-Fi** w naszym urządzeniu.
Po wyłączeniu GPS i Wi-Fi jedyną możliwością namierzenia smartfona jest śledzenie go przez dane mobilne lub numer telefonu przy wykorzystaniu stacji BTS. Trzeba by więc **wyłączyć funkcję danych mobilnych** i **wyjąć kartę SIM**. Dochodzimy jednak do absurdu, gdyż takie urządzenie na nic nam się nie przyda.
Musimy zaakceptować fakt, że w określonych okolicznościach będzie można namierzyć nasz smartfon.
Z drugiej strony, każdy z nas chciałby móc zlokalizować swoje urządzenie w przypadku, gdyby je zgubił lub zostało skradzione.



Namierzenie i blokowanie urządzenia po zgubieniu

Na wszelki wypadek, zawczasu, warto przygotować się na taką ewentualność, że zdarzy nam się zgubić smartfon lub ktoś go nam ukradnie. Możemy skorzystać ze specjalnych funkcji wbudowanych w nasze urządzenia.
Przeczytajmy, jak skorzystać z funkcji **Znajdź mój iPhone** przeznaczonej dla urządzeń z systemem iOS oraz **Znajdź moje urządzenie** – dla urządzeń z systemem Android. W przypadku gdy nie będziemy wiedzieli, gdzie jest nasz smartfon, te funkcje pozwalają zdalnie go zablokować – dzięki temu nasze dane będą bezpieczne.

Przygotowanie na wypadek utraty urządzenia z systemem iOS

Dla urządzeń Apple przeznaczona jest funkcja **Znajdź mój iPhone**. Funkcja ta umożliwia odnalezienie i ochronę takich urządzeń, jak: iPhone, iPad, iPod Touch, zegarek Apple Watch, słuchawki AirPods oraz MacBook.

Za jej pomocą można:

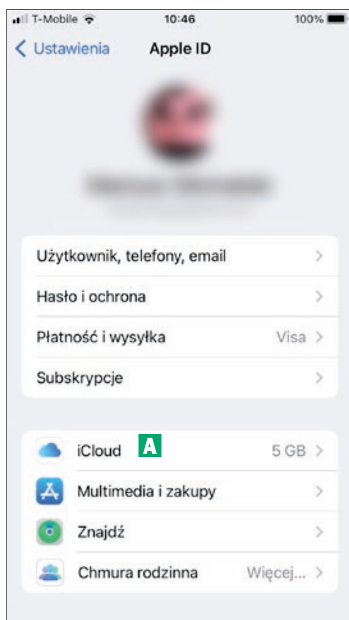
- odtworzyć dźwięk na urządzeniu, aby można było je łatwo odnaleźć,
- ustalić położenie na mapie,
- aktywować tryb **Utracony** w celu zablokowania i rozpoczęcia śledzenia urządzenia,
- zdalnie wymazać wszystkie osobiste informacje z urządzenia,
- włączyć ochronę urządzenia blokadą aktywacji.

Jak widzimy, możliwości jest sporo. Warto zadbać o to, aby poprawnie skonfigurować tę funkcję, by później móc z niej skorzystać.

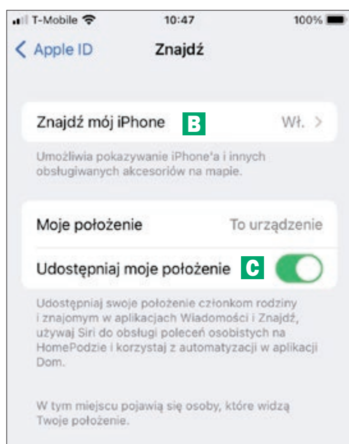
1 Na ekranie początkowym naciskamy **Ustawienia**, nasze imię i nazwisko, **iCloud** **A**.

2 Przewijamy ekran w dół i naciskamy opcję **Znajdź**.

adam13zajac@gmail.com



3 Przeciągamy, aby włączyć opcje **Znajdź mój iPhone** B oraz **Udostępniaj moje położenie** C.



4 Jeśli pojawi się monit z prośbą o zalogowanie z wykorzystaniem Apple ID, wprowadzamy potrzebne dane.

Warto wiedzieć: Jeżeli ze smartfonem mamy sparowany zegarek i słuchawki, funkcja Znajdź mój iPhone zostanie automatycznie włączona również dla tych urządzeń.

Wyszukujemy urządzenie za pomocą funkcji Znajdź mój iPhone

W przypadku gdy zgubimy nasze urządzenie lub zostanie ono skradzione, a wcześniej skonfigurowaliśmy funkcję Znajdź mój iPhone, to korzystając ze strony **iCloud.com**, możemy ustalić jego przybliżoną lokalizację i wykonać możliwe akcje.

1 Po wejściu na stronę **icloud.com/find** podajemy nasze Apple ID A i logujemy się.



2 Następnie klikamy na **Wszystkie urządzenia**. Kropka obok nazwy urządzenia informuje o jego stanie. Kolor zielony oznacza, że urządzenie jest aktywne i wyświetlana jest jego ostatnia znana lokalizacja. Kolor szary informuje o tym, że urządzenie jest nieaktywne.

3 Gdy wybierzemy urządzenie, które jest aktywne, na mapie zostanie wskazana jego aktualna pozycja. Możemy kliknąć na zielony punkt na mapie, a następnie na **Odśwież** w celu uaktualnienia położenia.

4 Z poziomu iCloud możemy również wykonać opisane wcześniej czynności, na przykład zdalnie wymazać dane. Należy jednak pamiętać, że czynność ta jest nieodwracalna i jeśli odzyskamy później nasze urządzenie, nie da się przywrócić danych.

adam13zajac@gmail.com

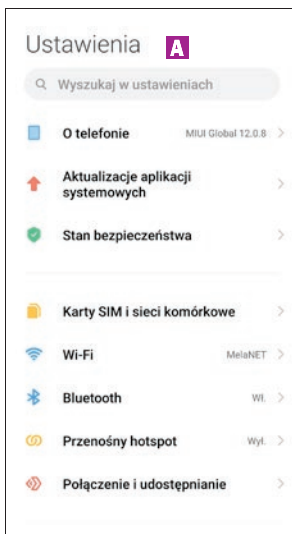
Przygotowanie na wypadek utraty urządzenia z systemem Android

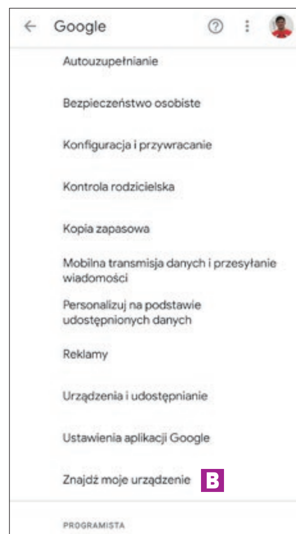
Użytkownicy urządzeń z systemem Android mogą skorzystać z bardzo podobnej funkcji jak użytkownicy urządzeń firmy Apple. Po skonfigurowaniu funkcji **Znajdź moje urządzenie** będziemy mogli namierzyć telefon, tablet, zegarek z Wear OS.

Opisane dalej kroki są przeznaczone dla posiadaczy urządzeń z systemem Android w wersji 8.0 i wyższych.

Funkcja Znajdź moje urządzenie po konfiguracji umożliwia korzystanie z takich opcji, jak:

- **Odtwórz dźwięk:** powoduje włączenie dzwonka na pięć minut przy maksymalnej głośności, nawet jeśli wcześniej był on wyciszony lub były włączone tylko wibracje.
- **Zabezpiecz urządzenie:** blokuje telefon kodem PIN, wzorem lub hasłem. Jeśli nie masz blokady, możesz ją ustawić. Aby pomóc komuś zwrócić ci telefon, do ekranu blokady możesz dodać wiadomość lub numer telefonu kontaktowego.
- **Wymaż urządzenie:** powoduje trwałe usunięcie wszystkich danych zapisanych na urządzeniu (ale może nie wykasować zawartości karty SD). Po wykasowaniu danych usługa Znajdź moje urządzenie nie będzie działać na telefonie.





A oto jak skonfigurować smartfon do korzystania z funkcji **Znajdź moje urządzenie**:

1 Na naszym urządzeniu otwieramy **Ustawienia** **A**.

2 Następnie przechodzimy do **Zabezpieczenia**, **Znajdź moje urządzenie**. Jeśli nie mamy opcji Zabezpieczenia, przechodzimy

JAKIE WARUNKI MUSZĄ BYĆ SPEŁNIONE, ABY DAŁO SIĘ ODNALEŹĆ URZĄDZENIE Z ANDROIDEM

Zarówno w przypadku urządzeń Apple, jak i tych pracujących z systemem Android muszą być spełnione konkretne warunki, aby dało się je odnaleźć. Na przykład aby można było odnaleźć czy zdalnie zablokować urządzenie z Androidem lub wymazać dane, muszą być spełnione następujące warunki:

- telefon musi być włączony,
- na telefonie musi być zalogowane konto Google,
- telefon musi mieć włączoną mobilną transmisję danych lub Wi-Fi,
- telefon musi być widoczny w Google Play,
- na telefonie musi być włączona lokalizacja,
- na telefonie musi być włączona usługa Znajdź moje urządzenie.

adam13zajac@gmail.com

do **Lokalizacja i blokady** lub **Google**, **Znajdź moje urządzenie** **B**.

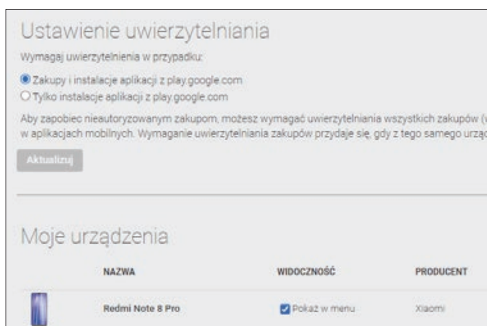
3 Teraz wystarczy aktywować tę funkcję.

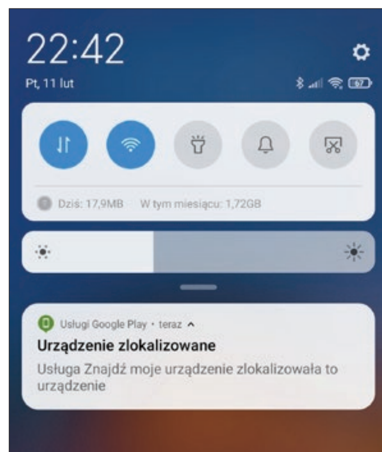


4 Następnie upewniamy się, że funkcja **Lokalizacja** jest aktywna.



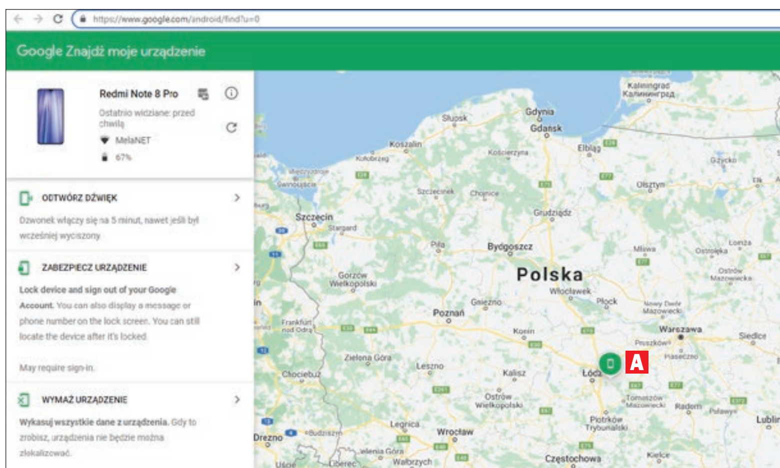
5 Teraz wchodzimy na **play.google.com/settings** i w sekcji **Moje urządzenia** w kolumnie **Widoczność** upewniamy się, że nasze urządzenie jest aktywne.
Po wykonaniu tych kroków będziemy mogli odnaleźć nasze urządzenie, gdy je zgubimy lub zostanie nam skradzione.





Odnajdywanie urządzenia z systemem Android

Jeśli skonfigurowaliśmy poprawnie funkcję **Znajdź moje urządzenie** i po jakimś czasie zdarzy nam się zgubić nasz sprzęt, będziemy mogli go wyszukać, zablokować, a nawet zdalnie wymazać. Oto, co trzeba zrobić, aby odnaleźć urządzenie.

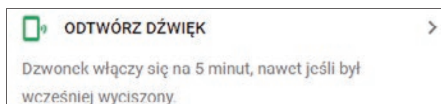


adam13zajac@gmail.com

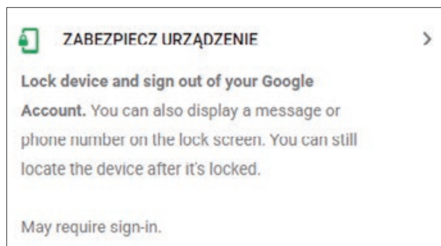
1 Wchodzimy na stronę **google.com/android/find** i logujemy się na to samo konto Google, na jakie byliśmy zalogowani na zgubionym urządzeniu. Po chwili na smartfonie pojawi się powiadomienie o zlokalizowaniu urządzenia.

2 Na stronie **google.com/android/find** będziemy mogli sprawdzić dokładną lokalizację urządzenia przedstawioną na mapie **A**. Jeżeli telefonu nie będzie można odnaleźć, zostanie wskazana jego ostatnia znana lokalizacja.

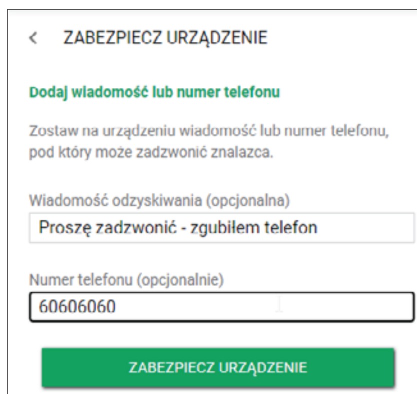
3 Po lewej stronie okna znajdziemy dodatkowe funkcje i akcje, jakie możemy wykonać zdalnie. W przypadku zgubienia urządzenia w domu warto kliknąć na opcję **Odtwórz dźwięk** – zostanie aktywowany dzwonek i nawet jeśli urządzenie było wyciszone, będzie on słyszalny.



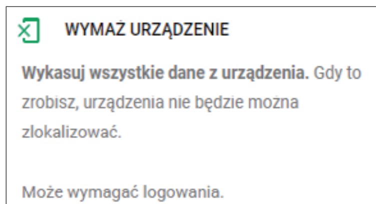
4 Możemy też kliknąć na **Zabezpiecz urządzenie**. Co ciekawe, możemy zablokować zdalnie nasz telefon i wyświetlić na ekranie blokady wiadomość lub numer telefonu kontaktowego. Jeśli nasze urządzenie znajdzie jakaś przypadkowa osoba, będzie mogła od razu zadzwonić pod podany numer i być może szybciej odzyskamy nasz telefon. Po podaniu opcjonalnych danych klikamy na **Zabezpiecz urządzenie**.



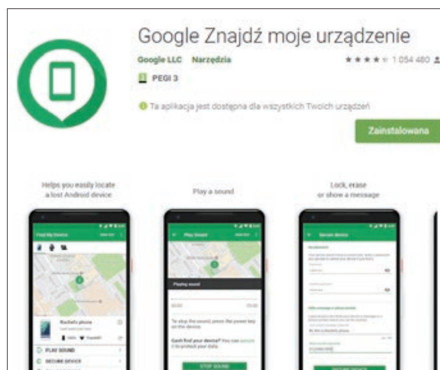
5 Ostatnia opcja to **Wymaż urządzenie** – opcja ta jest nieodwracalna i przywraca



telefon do stanu fabrycznego, usuwając z niego wszystkie osobiste informacje użytkownika. Używajmy jej tylko w ostateczności.

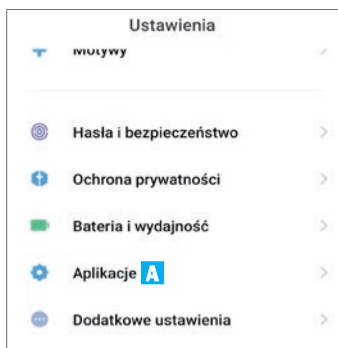


Warto wiedzieć: Alternatywnie możemy skorzystać z aplikacji ze sklepu Google Play – **Google Znajdź moje urządzenie**. Po zainstalowaniu jej na innym urządzeniu z Androidem będziemy mogli wykonywać te same operacje co na stronie internetowej. Jest to wygodne rozwiązanie w przypadku, gdy jesteśmy z dala od komputera.



Ochrona prywatności na smartfonie

Powszechna inwigilacja to coraz poważniejszy temat. Podsłuchiwanie i śledzenie dotyczy wielu urządzeń. Trudno znaleźć markę, która tworzy urządzenia w pełni bezpieczne, bez żadnych furtek dla służb bezpieczeństwa, a także dla hakerów. Nawet jeśli sam system jest odporny na inwigilację, wystarczy zainstalować jedną szkodliwą aplikację ze sklepu i nadać jej zbyt duże uprawnienia, a nasze dane zostaną przesłane na serwery firm trzecich.



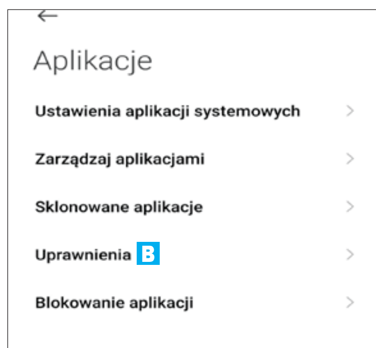
Uprawnienia aplikacji w Androidzie

Dobrą wiadomością jest to, że możemy łatwo zwiększyć nasze bezpieczeństwo, po prostu uważając podczas instalowania nowych aplikacji i przyznając im tylko uprawnienia, które są naprawdę niezbędne do działania. Warto też sprawdzić, jakie uprawnienia są przyznane już zainstalowanym aplikacjom.

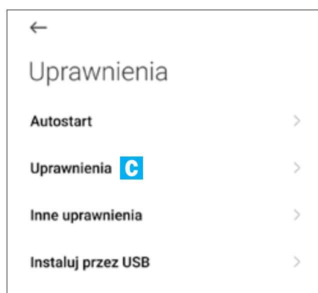
A jeśli część preinstalowanych aplikacji, z których korzystamy, nie zapewnia odpowiedniego stopnia prywatności, warto zmienić je na takie, które są bezpieczniejsze. Dobrym przykładem na to, że warto zwracać uwagę na uprawnienia aplikacji, są gry mobilne, które mają dodatkową funkcję czatu głosowego. Instalując taką grę, zostaniemy poproszeni o przyznanie jej dostępu do mikrofonu, aparatu i kontaktów. Z jednej strony taka prośba jest uzasadniona, ale z drugiej nie mamy pewności, kiedy gra będzie korzystać z naszego mikrofonu i czy nie będzie rejestrować wszystkich dźwięków w pobliżu naszego urządzenia. Dlatego decyzje o uprawnieniach należy podejmować rozważnie.

1 By sprawdzić i zmienić zmiany uprawnienia aplikacji, otwieramy **Ustawienia**, a potem wybieramy **Aplikacje** **A**.

2 Następnie przechodzimy do opcji **Uprawnienia** **B**.



3 Na kolejnym ekranie ponownie naciskamy pozycję **Uprawnienia** **C**.



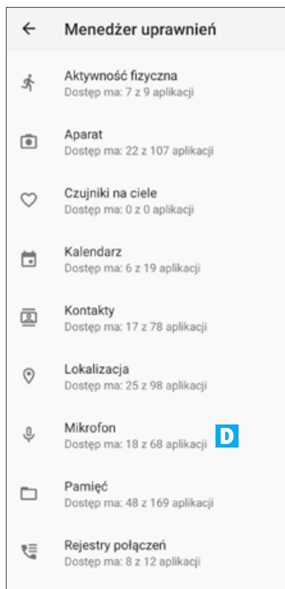
4 Zostanie uruchomiony **Menedżer uprawnień**. Teraz możemy naciskać poszczególne uprawnienia i sprawdzać, które aplikacje mają je przyznane. Wybierzmy na przykład pozycję **Mikrofon** **D**.

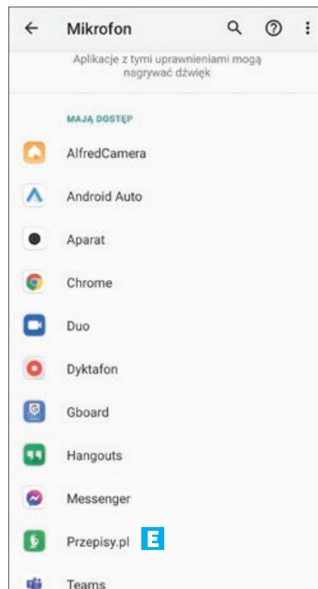
5 Na liście znajdziemy wszystkie aplikacje, które mają udzielony dostęp do mikro-

adam13zajac@gmail.com

fonu naszego urządzenia. Aparat czy aplikacje do komunikacji, w których często korzystamy z mikrofonu, nie powinny dziwić. Zaskakuje jednak to, że dostęp do mikrofonu ma aplikacja **Przepisy.pl** E, która służy do wyszukiwania przepisów kulinarnych. W tym wypadku powinniśmy zablokować dostęp, gdyż nie jest on niezbędny do działania aplikacji. W ten sposób możemy ręcznie sprawdzić wszystkie uprawnienia aplikacji na naszym urządzeniu.

6 Aby cofnąć uprawnienia, naciskamy wy-





DO CZEGO SŁUŻĄ POSZCZEGÓLNE UPRAWNIENIA

Tutaj umieściliśmy kompletną listę uprawnień w systemie Android wraz z opisem, co powoduje przyznanie konkretnego uprawnienia aplikacji.

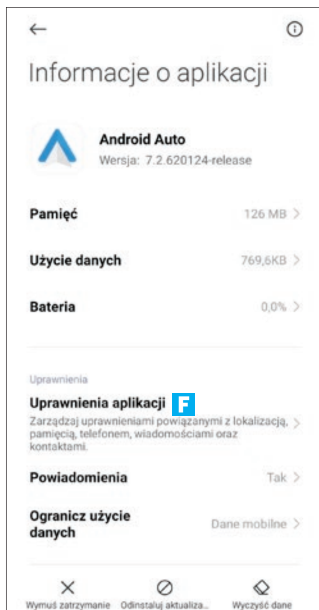
- **Czujniki na ciele:** otrzymuje dane czujnika podstawowych funkcji życiowych.
- **Kalendarz:** używa twojego domyślnego kalendarza.
- **Rejestry połączeń:** wyświetla i edytuje historię połączeń.
- **Aparat:** używa aparatu do robienia zdjęć i nagrywania filmów.
- **Kontakty:** wyświetla listę kontaktów.
- **Lokalizacja:** prosi o udzielenie informacji o lokalizacji urządzenia.
- **Mikrofon:** nagrywa dźwięk.
- **Urządzenia Bluetooth w pobliżu:** aplikacje mogą wykrywać urządzenia w pobliżu i łączyć się z nimi.
- **Telefon:** nawiązuje połączenia telefoniczne i zarządza nimi.
- **Aktywność fizyczna:** odbiera informacje o twojej aktywności, takiej jak chodzenie, jazda na rowerze, liczba kroków itp.
- **SMS:** wyświetla i wysyła SMS-y.
- **Pamięć:** pobiera zdjęcia i inne pliki na telefon.
- **Pliki i multimedia:** korzysta ze zdjęć, multimediów i innych plików na telefonie.

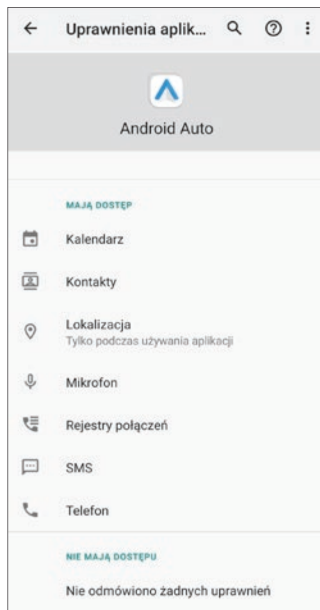
W zależności od aplikacji, jakie mamy na naszym urządzeniu, możemy znaleźć dodatkowe uprawnienia, na przykład dostęp do wiadomości e-mail, dostęp do informacji o aucie i inne.

adam13zajac@gmail.com

braną aplikację, a następnie zmieniamy opcję **Zezwól** na **Odmów**.

Warto wiedzieć: Możemy również na pierwszym ekranie po naciśnięciu pozycji **Aplikacje** wybrać opcję **Zarządzaj aplikacjami**, a następnie wskazać konkretną aplikację i wybrać **Uprawnienia aplikacji** F. W tym widoku będziemy mieli dostęp do wszystkich uprawnień, jakie zostały przyznane danej aplikacji. Można wygodnie wybierać poszczególne uprawnienia i zmieniać ich status.





Aplikacja dla wygodnych – Paranoid for Android

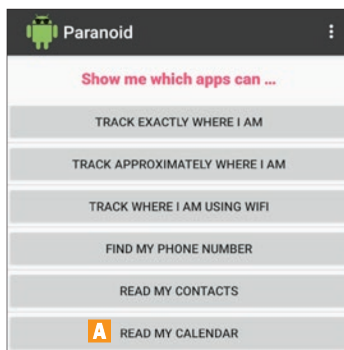
Jeżeli opisany proces wydaje nam się zbyt czasochłonny, w wypadku urządzeń z Androidem możemy skorzystać z bezpiecznej aplikacji **Paranoid for Android**. Analizuje ona wszystkie zainstalowane na naszym smartfonie aplikacje i grupuje je według uprawnień, które są im aktualnie przyznane – pozwala namierzyć aplikacje, które mogą nas podsłuchiwać, podglądać, śledzić, dzwonić w naszym imieniu lub wydawać pieniądze. Dodatkowo, aby pomóc mniej doświadczonym użytkownikom, Paranoid for Android zaznacza, które z uprawnień według kryteriów Androida są niebezpieczne, i umożliwia szybkie przejście do ustawień, gdzie każde z uprawnień można łatwo wyłączyć.

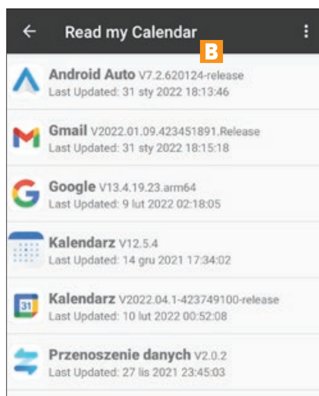


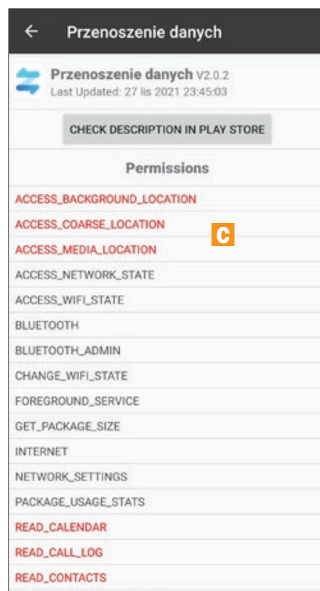
Korzystamy z Paranoid for Android

1 Po uruchomieniu aplikacji możemy wybrać jeden z dostępnych typów uprawnień, na przykład **Read my Calendar** A.

2 Po chwili zostanie przedstawiona lista aplikacji, które mają dostęp do naszego kalendarza B (następna strona).







3 Po przytrzymaniu palca dłużej na konkretnej aplikacji zostanie wyświetlona lista wszystkich przyznanych jej uprawnień. Kolorem czerwonym **C** są zaznaczone uprawnienia bardzo ważne, które potencjalnie zagrażają naszej prywatności.

4 Jeśli chcemy zablokować konkretne uprawnienia, wystarczy, że wskażemy aplikację, wybierzemy **Uprawnienia aplikacji** i wyłączymy zbędne uprawnienia.

Prywatność a przeglądarka

Zdecydowana większość użytkowników korzysta do przeglądania internetu na smartfonie z aplikacji Chrome. Warto jednak rozważyć alternatywę, czyli przeglądarkę **DuckDuckGo Privacy Browser**. Korzystając z niej, możemy być pewni, że nie zostawimy w sieci po sobie żadnych śladów i nie damy się śledzić dodatkom reklamowym. W każdej chwili możemy też wyczyścić sesję przeglądania i rozpocząć nową, czystą sesję. Ciekawą opcją dla osób bardzo wymagających jest możliwość automatycznego czyszczenia danych przeglądania po określonym czasie braku aktywności użytkownika. **Uwaga!** Pamiętajmy, aby w tej przeglądarce korzystać z silnika DuckDuckGo, a nie silnika Google, gdyż wtedy nasze wyszukiwania będą zapisywane.

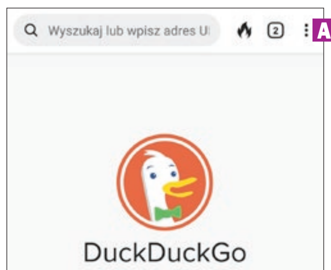


Konfiguracja DuckDuckGo Privacy Browser i korzystanie z aplikacji

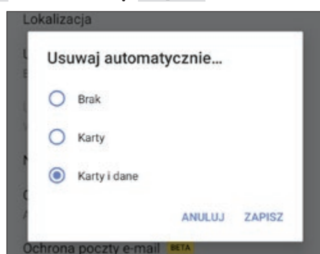
1 Po uruchomieniu przeglądarki możemy od razu aktywować funkcję automa-

adam13zajac@gmail.com

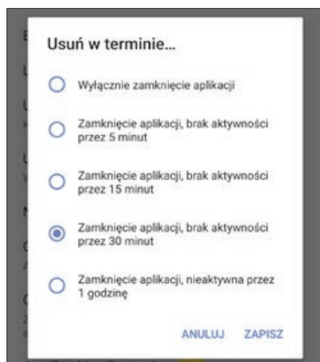
tycznego czyszczenia danych. W głównym oknie programu naciskamy trzy kropki **A** w prawym górnym rogu ekranu, a następnie **Ustawienia**.



2 W ustawieniach naciskamy **Usuwaj automatycznie**, wybieramy opcję **Karty i dane** i naciskamy **Zapisz**.



3 Następnie naciskamy **Usuń w terminie** i wybieramy odpowiadającą nam opcję. Na koniec naciskamy **Zapisz**.



4 Z aplikacji możemy korzystać zupełnie normalnie, jak z innych przeglądarek. Na górnym pasku możemy wyszukiwać różne frazy lub podawać bezpośrednio adresy stron. Po przejściu na dowolną stronę w lewym górnym rogu zostanie wyświetlona informacja z oceną prywatności danej strony.



5 Po naciśnięciu symbolu oceny będziemy mogli zapoznać się ze szczegółami. Jak



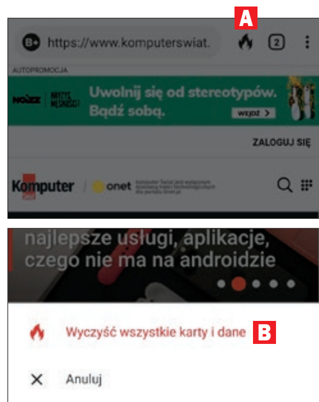
widać witryna **komputerswiat.pl** uzyskała ocenę **B+**. Jest to bardzo wysoka ocena. Dzięki systemowi rozszyfrowywania polityk prywatności DuckDuckGo jest w stanie bardzo szybko podać szczegółowe informacje na temat ochrony prywatności na konkretnej

adam13zajac@gmail.com

witrynie. Dzięki temu, odwiedzając witrynę, od razu wiemy, czy możemy czuć się na niej bezpiecznie.

Czyszczenie sesji w DuckDuckGo Privacy Browser

W celu szybkiego wyczyszczenia sesji i wszystkich danych przeglądania wystarczy nacisnąć ikonę płomienia **A** po prawej stronie paska adresowego. Następnie naciskamy **Wyczyść wszystkie karty i dane** **B**. Pojawi się animacja płomieni i wszystkie dane przeglądania zostaną usunięte.



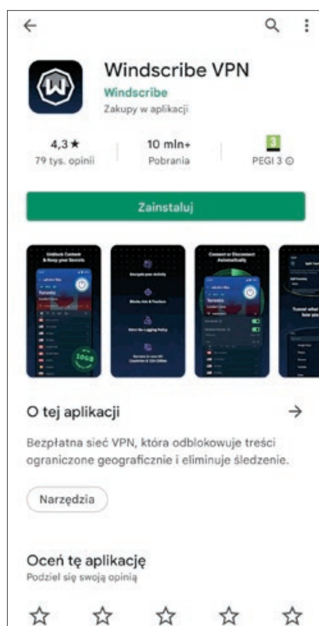
VPN dla smartfona

Świetnym uzupełnieniem przeglądarki, która dba o naszą prywatność, jest korzystanie na urządzeniu mobilnym z programów typu VPN. Jest to nawet bardziej wskazane niż w przypadku komputera, gdyż właśnie używając smartfonów, bardzo często łączymy się z potencjalnie niebezpiecznymi otwartymi sieciami Wi-Fi oraz takimi, do których każdy może mieć dostęp (na przykład w miejscach publicznych) i w każdej chwili może bez naszej wiedzy przejąć nasze dane. Tryb incognito, który oferują przeglądarki, pozwala jedynie wymazać historię przeglądania z naszego urządzenia. A ruch sieciowy, jeśli nie będzie zaszyfrowany, może zostać odczytany przez osoby trzecie, które mogą uzyskać w ten sposób dostęp do naszych prywatnych danych.

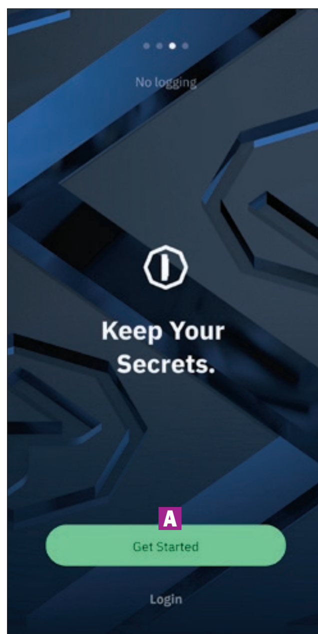
W przypadku korzystania z usługi VPN na telefonie po pierwsze jesteśmy chronieni, gdyż połączenie jest szyfrowane i zwykli użytkownicy nie będą mogli nas podsłuchać, a po drugie, będąc w podróży, możemy zawsze połączyć się z serwerami w kraju, z którego treści chcemy oglądać.

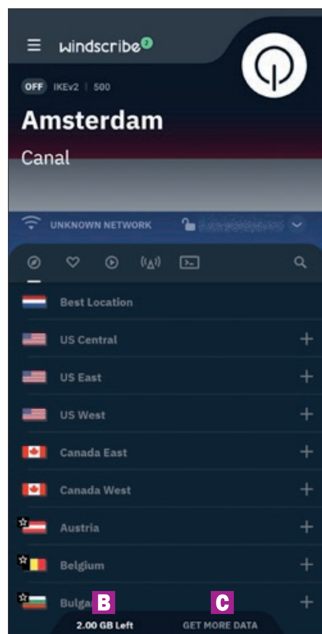
Warto tylko pamiętać o tym, że jeśli korzystamy z bankowości internetowej przez VPN i często zmieniamy zagraniczne serwery, proces logowania może zostać automatycznie zablokowany ze względu na próby dostania się na nasze konto z różnych krajów w krótkim czasie. Ale przy logowaniu z włączoną usługą VPN i nawiązanym połączeniem z serwerem w Polsce taki problem nie powinien występować.

Aplikacje oferujące usługi VPN możemy instalować zarówno na urządzeniach z systemem Android, jak i iOS.



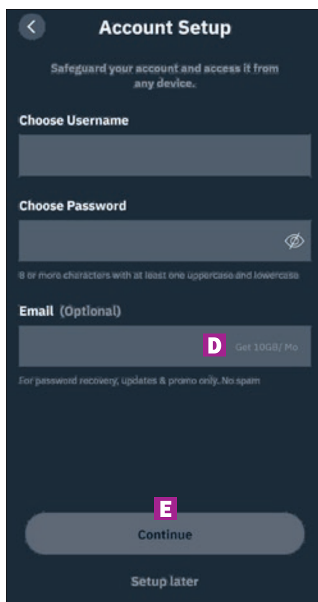
A z jakiej aplikacji VPN najlepiej korzystać? Polecane są takie VPN-y, które oferują szyfrowanie 256-bit i sprawdzony protokół, na przykład OpenVPN.
Dodatkowo, jeśli zależy nam na korzystaniu z VPN i jednocześnie ochronie prywatności, warto zweryfikować, co usługodawca może zrobić z naszymi danymi. Część usługodawców rejestruje aktywność użytkowników i może zbierać dane o nich, aby później sprzedawać te informacje reklamodawcom.
Kolejnym ważnym aspektem jest przepustowość łącza oferowanego w ramach usługi oraz ilość dostępnych serwerów i ich lokalizacja.
Ostatnim wartym sprawdzenia parametrem jest limit transferu danych – w darmowych wersjach usługodawcy zapewniają często jedynie kilkaset megabajtów transferu, co może nie być wystarczające dla użytkowników aktywnie korzystających z internetu.





Windscribe VPN

Windscribe to markowy VPN, który w podstawowej, darmowej wersji udostępnia bezpłatny pakiet danych 10 GB miesięcznie. Program ma prosty, nowoczesny interfejs i wersje na wszystkie popularne platformy. Windscribe oferuje silne szyfrowanie połączenia z internetem, aby przesyłane przez nas informacje nie mogły być odczytane przez dostawcę usług internetowych ani operatora sieci Wi-Fi. Chroni również naszą prywatność. Nie tylko ukrywa nasz adres IP, co pozwala omijać różnego typu internetowe blokady i anonimowo publikować w sieci, ale ma również funkcje do blokowania trackerów, malware'u i reklam.



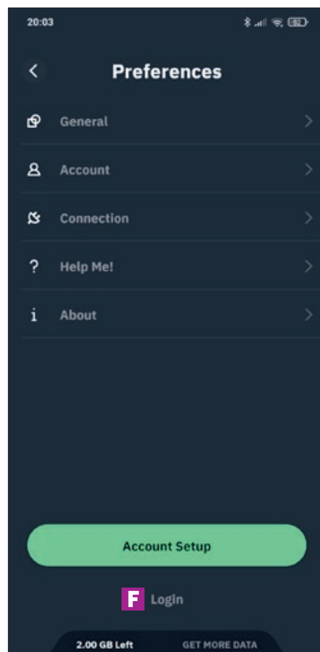
Do konta użytkownika nie ma przypisanego limitu urządzeń.

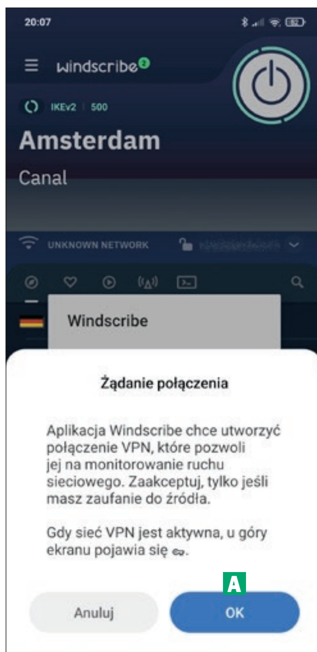
1 Instalujemy Windscribe VPN, uruchamiamy go i klikamy na **Get Started** **A**.

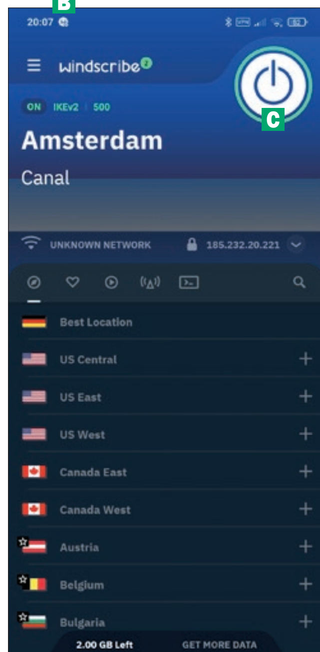
2 Otrzymamy do wykorzystania 2 GB miesięcznie bez konieczności zakładania konta. Ilość dostępnych danych do wykorzystania jest prezentowana na dolnym pasku w oknie aplikacji **B**.

3 Jeśli chcemy zwiększyć tę ilość do 10 GB miesięcznie, wystarczy kliknąć na **Get More Data** **C**, a następnie na **Get Free 10GB/**

adam13zajac@gmail.com







Month D. Przechodzimy do zakładania konta. Podajemy nazwę użytkownika, hasło oraz adres e-mail i wybieramy **Continue** E.

4 Po przejściu przez opisaną procedurę musimy jeszcze kliknąć na link aktywacyjny, jaki zostanie wysłany na nasz adres e-mail. Następnie w głównym oknie aplikacji naciskamy w lewym górnym rogu trzy kreski, a potem **Login** F.

5 Podajemy nasze dane i po chwili możemy rozpocząć korzystanie z programu.

Korzystamy z Windscribe VPN

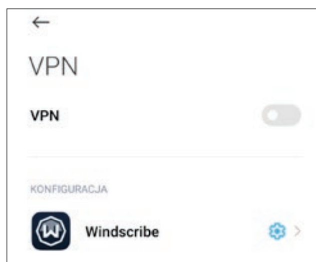
1 W celu aktywowania usługi VPN należy z listy wybrać serwer, z którym chcemy się połączyć. Potem naciskamy ikonę włączania w górnym prawym rogu. Po chwili pojawi się prośba o nawiązanie połączenia – naciskamy **OK** A.

2 Po poprawnym nawiązaniu połączenia interfejs programu zmieni kolor na niebieski, a na górnym pasku naszego urządzenia pojawi się ikona klucza lub ikona Windscribe VPN B, co oznacza, że nasze połączenie z internetem jest szyfrowane.

3 W celu zakończenia połączenia VPN należy ponownie nacisnąć **ON/OFF** C.

Automatyczne włączanie VPN przy uruchamianiu smartfona

Jeśli zależy nam, aby ruch sieciowy był szyfrowany już od razu po uruchomieniu smart-

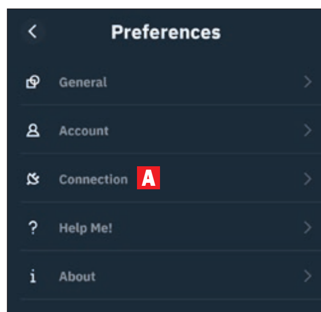


Warto wiedzieć, że gdy wyrazimy zgodę na pierwsze nawiązanie połączenia w aplikacji, automatycznie stworzona zostanie konfiguracja połączenia VPN dla Windscribe VPN w ustawieniach naszego urządzenia, gdzie możemy sami zarządzać powiązanymi opcjami

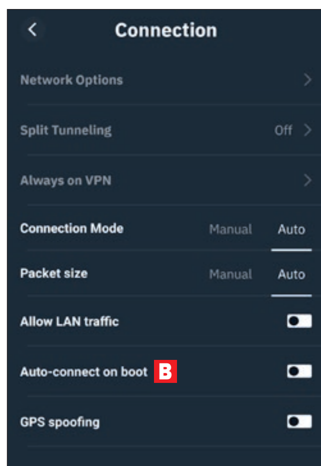
adam13zajac@gmail.com

fona, warto włączyć odpowiednią opcję w ustawieniach aplikacji **Windscribe VPN**.

1 Po uruchomieniu aplikacji przechodzimy do opcji, naciskając trzy kreski w lewym górnym rogu, a następnie **Connection** **A**.

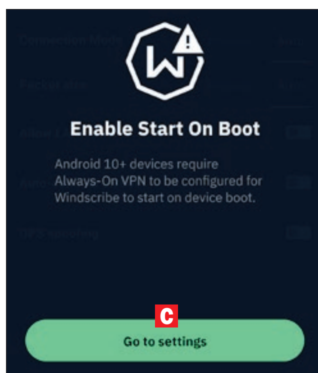


2 Potem aktywujemy funkcję **Auto--connect on boot** **B**.

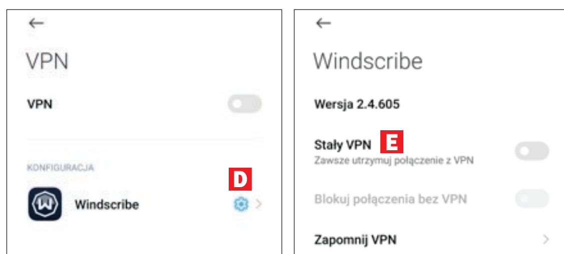


3 Przy próbie włączenia tej opcji na urządzeniu z systemem Android w wersji 10 i wyższej pojawi się informacja o potrzebie konfiguracji w ustawieniach systemu – klikamy na **Go to settings** **C**.

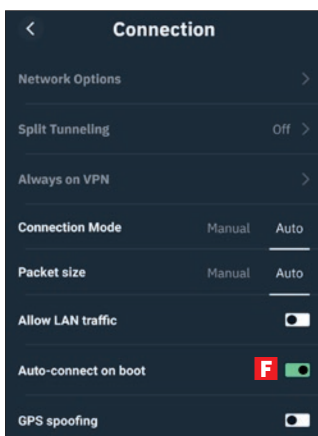
4 Następnie naciskamy ikonę koła zębatego przy opcjach konfiguracji programu Windscribe **D**.



5 Teraz wystarczy aktywować opcję **Stały VPN** **E**.



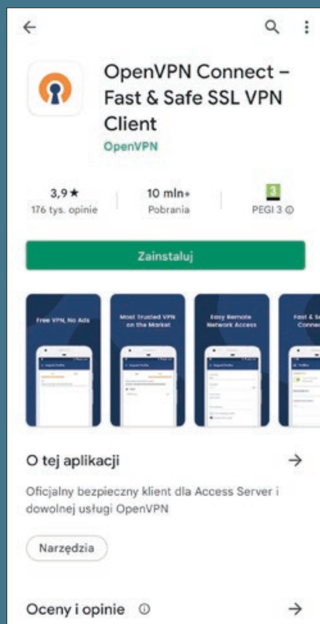
6 Po powrocie do aplikacji Windscribe będziemy mogli aktywować funkcję **Auto-connect on boot** **F** i cieszyć się prywatnością w każdej chwili działania naszego urządzenia.



adam13zajac@gmail.com

KONFIGURUJEMY POŁĄCZENIE ZA POMOCĄ OPENVPN

Opisany wcześniej program – Windscribe VPN – korzysta z protokołu IKEv2, nie jest on natywnie wspierany przez system Android, jednak dzięki specjalnemu API dla deweloperów twórcy aplikacji mogą wykorzystać dowolny protokół do świadczenia usługi VPN w systemie Android. Korzystając z tej funkcjonalności, możemy

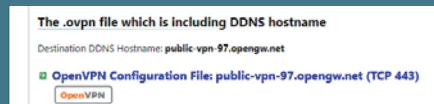


ręcznie dodać konfigurację dla protokołu OpenVPN, który zapewnia bardzo wysoki poziom bezpieczeństwa i korzysta z niego bardzo wielu pracodawców. Dzięki poprawnej konfiguracji będziemy mogli na przykład uzyskać dostęp do służbowych zasobów bezpośrednio z poziomu naszego smartfona, łącząc się z firmowym serwerem VPN.

Proces konfiguracji wymaga od użytkownika plików konfiguracyjnych w formacie **OVPN**. Należy umieścić je w pamięci smartfona – możemy po prostu pobrać je z internetu lub przesłać z komputera. Następnie musimy zainstalować aplikację **OpenVPN Connect**.

1 W celu przetestowania działania usługi VPN z protokołem OpenVPN na smartfonie można pobrać pliki konfiguracyjne z jednego z dostępnych serwerów na stronie **vpngate.net/en**. W przypadku wszystkich serwerów domyślna nazwa użytkownika i hasło to **vpn**. Wybieramy jeden z serwerów i klikamy na **OpenVPN Config file** **A**.

2 Następnie pobieramy plik konfiguracyjny z rozszerzeniem OVPN i zapisujemy w pamięci naszego smartfona.



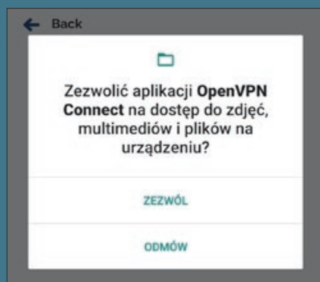
3 Po zainstalowaniu aplikacji OpenVPN Connect uruchamiamy ją na naszym urządzeniu. Na etapie importowania profilu

Do you want to parse the below HTML table? Instead you can use **CSV List** to make your own VPN Gate client app.

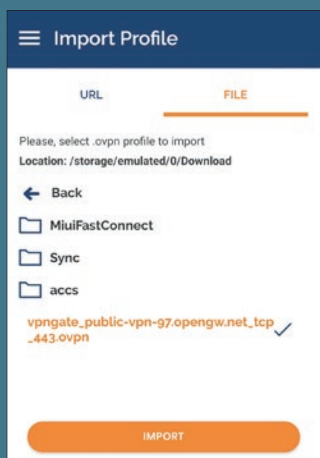
Country (Physical location)	DDNS hostname IP Address (ISP hostname)	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative transfers Logging policy	SSL-VPN Windows (comfortable)	L2TP/IPsec Windows, Mac, iPhone, Android No client required	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT No client required
Japan	**public-vpn-97.opengw.net** 219.100.37.83 (public-vpn-06-03.vpngate.v4.open.ad.jp)	**94 sessions** 9 days Total 4,641,177 users	**1,657.59 Mbps** Ping: 13 ms 195,597.96 GB Logging policy: 2 Weeks	✓ SSL-VPN Connect guide TCP: 443 UDP: Supported	✓ L2TP/IPsec Connect guide	✓ OpenVPN Config file TCP: 443 **A**	✓ MS-SSTP Connect guide SSTP Hostname : public-vpn-97.opengw.net

adam13zajac@gmail.com

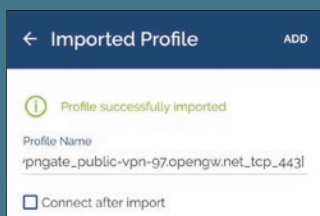
przechodzimy do zakładki **File** i przyznajemy dostęp do danych na urządzeniu.



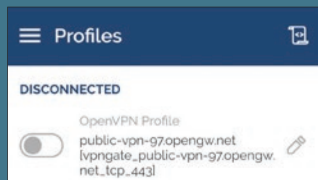
4 Następnie przechodzimy do lokalizacji, w której zapisaliśmy plik konfiguracyjny z rozszerzeniem **OVPN**, wybieramy go i klikamy na **Import**.



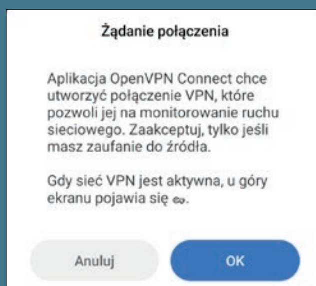
5 Po poprawnym zaimportowaniu profilu naciskamy w górnym prawym rogu **Add**.



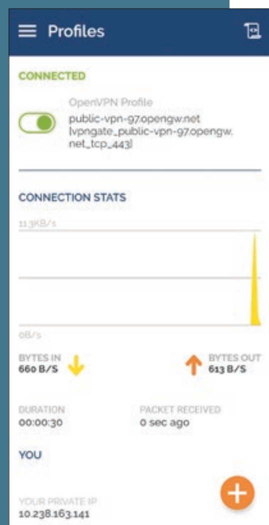
6 Teraz w widoku profili przełączamy szary włącznik w celu nawiązania połączenia VPN.



7 Wyrażamy zgodę na nawiązanie połączenia, naciskając **OK**.



8 Po chwili połączenie zostanie nawiązane – znacznik zmieni kolor na zielony. Dodatkowo będziemy mogli zapoznać się z wszystkimi dotyczącymi go danymi.



9 Dzięki obsłudze profili możemy w bardzo wygodny sposób przesłać na smartfon poprawną konfigurację z komputera i w kilka chwil nawiązać poprawne połączenie z serwerem VPN.

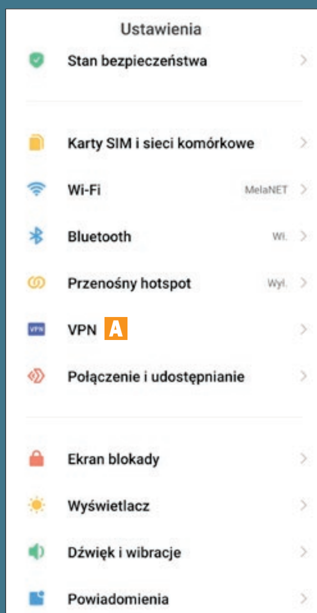
Cały proces jest bardzo podobny w przypadku urządzeń z systemem iOS.

DLA ZAAWANSOWANYCH

KONFIGURUJEMY POŁĄCZENIE VPN

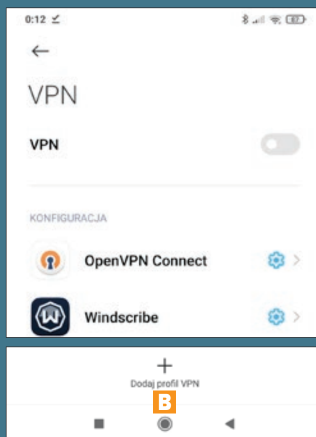
Zarówno w urządzeniach z Androidem, jak i iOS możemy również całkowicie ręcznie dodać konfigurację połączenia VPN bez konieczności instalacji jakichkolwiek aplikacji. Wystarczy, że będziemy znali dane serwera i typ protokołu.
Oto skrócony opis procesu na przykładzie Androida.

1 Przechodzimy do ustawień systemu i naciskamy **VPN** **A**; opcja ta może być również w: **Ustawienia**, **Sieci zwykłe i bezprzewodowe**, **Więcej**, **VPN**.

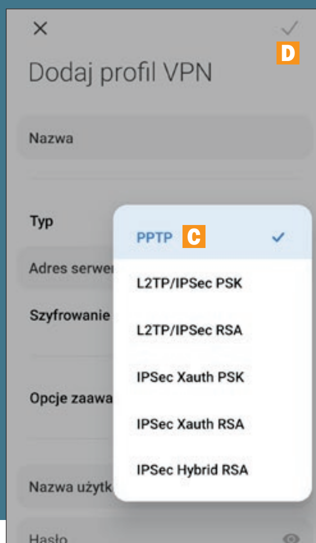


2 Następnie naciskamy **Dodaj profil VPN** **B** u dołu ekranu.

3 Podajemy nazwę dla naszego połączenia, wybieramy typ połączenia (protokół) **C**; iOS pozwala domyślnie skorzystać również z **IKEv2**. Następnie adres serwera, nazwę użytkownika i hasło. Pamiętamy o zapisaniu profilu przez naciśnięcie ikony akceptacji w górnym prawym rogu ekranu **D**.



Zaletą ręcznej konfiguracji połączenia VPN jest możliwość korzystania z funkcjonalności VPN bez konieczności instalowania aplikacji firm trzecich. Minusem jest brak możliwości użycia dowolnego protokołu i dostępu do zaawansowanych funkcji, jak szybka zmiana serwera i tym podobne.



adam13zajac@gmail.com

Bezpieczny komunikator

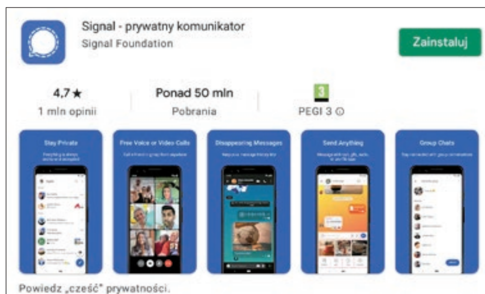
Jedno z podstawowych zastosowań smartfona to komunikacja z innymi. Warto zwrócić uwagę, z jakich aplikacji do komunikacji korzystamy. Zwykłe komunikatory, które udostępniane są przez największe sieci społecznościowe, nie są zbyt bezpieczną formą kontaktu, gdyż nasze dane mogą być przetwarzane na potrzeby silników reklamowych i nie tylko. Warto wybrać komunikator, który zapewni nam bezpieczeństwo poprzez szyfrowanie naszych rozmów, a jednocześnie prywatność – to znaczy nie będzie zbierał danych o nas. Takie godne zaufania komunikatory to **Signal** oraz **Telegram**. Ten pierwszy jest polecany przez Edwarda Snowdena – eksperta w dziedzinie prywatności.

Korzystamy z Signala

Signal pozwala na wysyłanie wiadomości tekstowych, obrazów, komunikację głosową, a także wideorozmowy. Cała komunikacja jest zabezpieczona – nikt nie będzie mógł nas podsłuchać ani podejrzeć, o czym piszemy. Dodatkowo możemy ustawić czyszczenie historii rozmów, dzięki czemu starsze wiadomości same będą znikały i nawet jeśli ktoś przejmie nasz smartfon, nie będzie mógł ich zobaczyć.

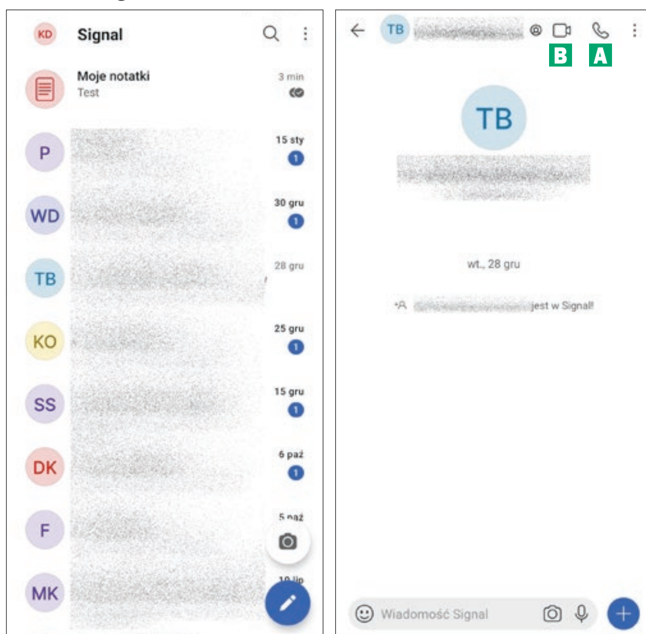
1 Po zainstalowaniu aplikacji ze sklepu uruchamiamy ją i przechodzimy wstępną konfigurację. Chwilę później pojawi się lista wszystkich naszych znajomych, którzy również mają Signala.

2 W celu rozpoczęcia rozmowy wystarczy wybrać kontakt i rozpocząć czat, tak jakbyśmy zrobili to w dowolnym innym komunikatorze. Możemy również, korzystając



z ikon w górnym prawym rogu ekranu, rozpocząć rozmowę głosową **A** lub wideopołączenie **B**.

3 Możemy wygodnie przesyłać pliki, zdjęcia i inne dane. Cała komunikacja jest szyfrowana. Jest to bardzo dobry sposób na bezpieczne przesyłanie danych – nasz dostawca internetu oraz operator nie będą w stanie sprawdzić, jakie dane przesyłamy.



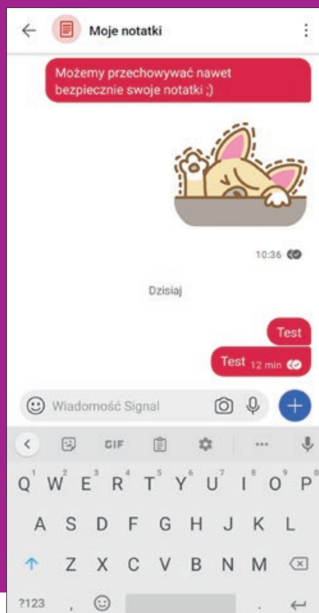
adam13zajac@gmail.com

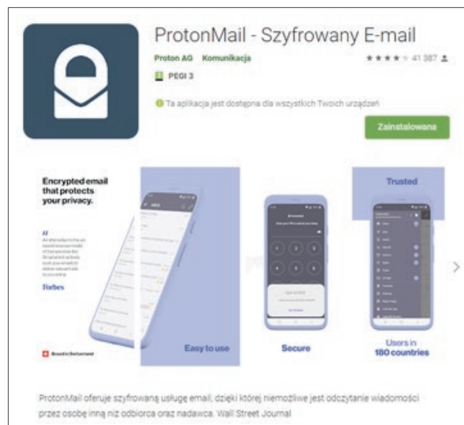
Bezpieczna i prywatna poczta e-mail

Coraz więcej osób aktywnie przegląda wiadomości e-mail na smartfonach. Ekrany urządzeń mobilnych są coraz większe i wygodnie jest szybko sprawdzić ważne e-maile. Problem może pojawić się wtedy, gdy zaczniemy szukać aplikacji mobilnej do obsługi poczty, która zapewni nam prywatność i bezpieczeństwo. Zdecydowana większość użytkowników korzysta z klientów Gmail oraz Outlook. Zarówno jedna, jak i druga aplikacja zbiera informacje o użytkownikach i nie zapewnia pełnego szyfrowania wiadomości. Jeśli zależy nam na najwyższym poziomie ochrony poczty, warto zapoznać się z **ProtonMail**.

ZASZYFROWANE NOTATKI

W Signalu mamy możliwość przechowywania własnych notatek. Wystarczy na liście kontaktów wybrać kontakt o nazwie Moje notatki. Następnie możemy wprowadzać wiadomości o dowolnej treści, które zostaną zaszyfrowane. Wszelkie dane zapisane w tej konwersacji są synchronizowane z naszym kontem i będziemy mieli do nich dostęp na dowolnym urządzeniu po zalogowaniu się na nasze konto.

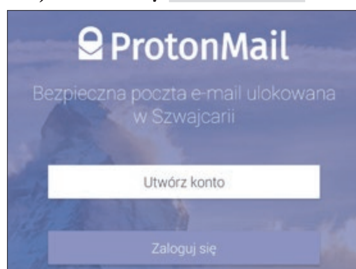




Konfiguracja wstępna w ProtonMail

ProtonMail to usługa bezpiecznej szyfrowanej poczty e-mail, która zadebiutowała w Szwajcarii ponad siedem lat temu. W darmowej wersji dostępnej dla każdego należy pamiętać o limicie pojemności głównej skrzynki (500 MB) oraz limicie 150 wiadomości dziennie. Na potrzeby prywatnego użytkownika to z reguły w zupełności wystarcza.

1 Po zainstalowaniu i uruchomieniu aplikacji naciskamy **Utwórz konto**.



adam13zajac@gmail.com

2 W kolejnym oknie otwieramy zakładkę **Free** i naciskamy **Zaznacz**.

ProtonMail

Wybierz typ konta

ProtonMail to darmowa usługa dla dobra publicznego. Wybierając płatne konto, wspierasz ochronę prywatności w sieci.

FREE

Podstawowe konto z ograniczoną liczbą funkcji –

- ✓ 500 MB przestrzeni dyskowej
- ✓ 150 wiadomości dziennie
- ✓ 20 etykiet
- ✗ Niestandardowe domeny: nie są obsługiwane
- ✓ 1 adres
- ✓ Wsparcie klienta: ograniczone

Zaznacz

3 Następnie podajemy nazwę naszego użytkownika i naciskamy **Utwórz konto**.

ProtonMail

Utwórz konto

krzysi @protonmail.com

Uwaga: Nazwa użytkownika jest również Twoim adresem ProtonMail

Korzystając z poczty ProtonMail, akceptujesz nasz regulamin oraz politykę prywatności

Utwórz konto

4 Na kolejnym ekranie ustalamy hasło do naszego konta i naciskamy **Ustaw hasło**.

5 Teraz wystarczy nacisnąć **Kontynuuj** i przejść weryfikację antyspamową w dowolny sposób i na koniec nacisnąć **Przejdź do mojej skrzynki**.

ProtonMail

Utwórz hasło

Uwaga: Służy do szyfrowania i odszyfrowywania Twoich wiadomości. Nie strać tego hasła - nie możemy go odzyskać. Jeśli je zgubisz, nie będziesz w stanie odczytać swoich wiadomości.

Ustaw hasło

ProtonMail

Weryfikacja antyspamowa

Aby zapobiec nadużyciom poczty ProtonMail, musimy zweryfikować, czy jesteś człowiekiem.

Wybierz jedną z następujących opcji:

CAPTCHA

Weryfikacja adresu e-mail

Weryfikacja przez telefon

Korzystamy z bezpiecznych wiadomości

1 W widoku skrzynki będziemy mieli dostęp do wszystkich naszych wiadomości. W celu wysłania nowej bezpiecznej wiadomości należy nacisnąć ikonę długopisu w prawym górnym rogu.

ODEBRANE

Get started with ProtonMail and increase your storag... 02:07
Proton Team

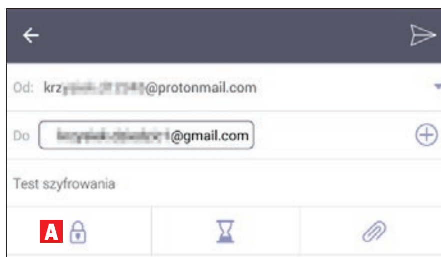
Welcome to the future of email 02:07
Proton Team

How to secure your ProtonMail account 02:07
Proton Team

Encrypt your Internet with ProtonVPN 02:07
Proton Team

adam13zajac@gmail.com

2 **Uwaga!** W pełni szyfrowane end-to-end są jedynie wiadomości, które wymieniane są pomiędzy użytkownikami ProtonMail. Jeśli zamierzamy wysłać wiadomość na przykład do użytkownika poczty Gmail, należy nacisnąć kłódkę **A**.



3 Następnie dwukrotnie podajemy hasło wiadomości i naciskamy **Zastosuj** **B**.

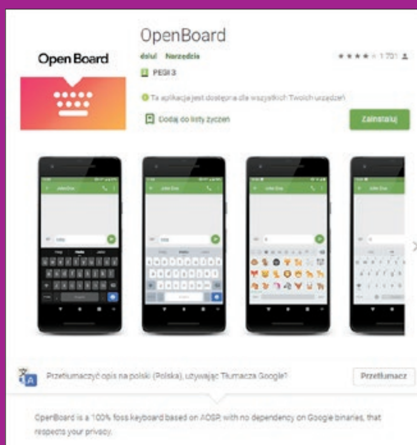
4 Po wysłaniu wiadomości nasz odbiorca otrzyma zaszyfrowaną wiadomość. W celu jej odczytania będzie musiał nacisnąć **View Message** **C**.

KLAWIATURA DO ZADAŃ SPECJALNYCH

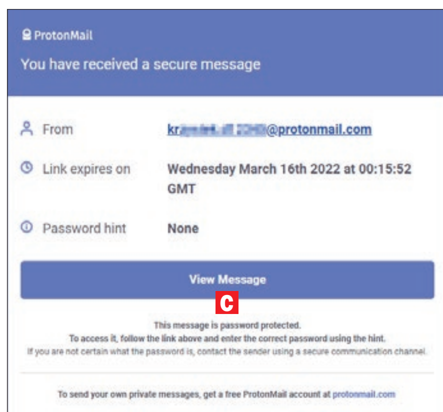
Jeśli do tematu prywatności podchodzimy bardzo poważnie i chcemy być w stu procentach zabezpieczeni przed wyciekiem danych, warto rozważyć korzystanie z bezpiecznej aplikacji klawiatury. Te najpopularniejsze zbierają dane o użytkownikach. Tymczasem są aplikacje, które umożliwiają wprowadzanie tekstu na smartfonie, nie pobierając żadnych danych.

Należy jednak rozważyć, czy będziemy chcieli zrezygnować z wygody na rzecz prywatności. Podstawową zaletą popularnych apek klawiaturowych, takich jak Klawiatura Google lub SwiftKey, jest to, że mają takie funkcje, jak: podpowiadanie kolejnego słowa, automatyczna korekta czy pisanie poprzez przeciąganie – dzięki temu, że zapamiętują dane.

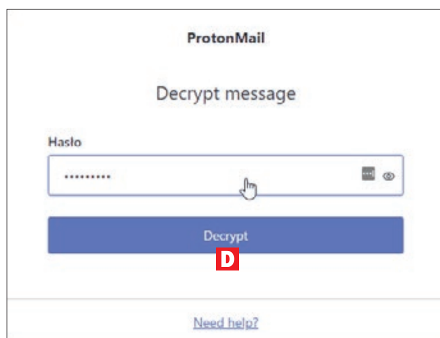
Jeśli jednak jesteśmy skłonni zrezygnować z tych opcji, warto zainstalować na przykład OpenBoard. Dobrym wyjściem może być korzystanie z tej klawiatury tylko wtedy, gdy naprawdę będzie zależało nam na prywatności. Warto wiedzieć, że OpenBoard, jako jedna z nielicznych klawiatur dbających o prywatność, ma funkcję autokorekty.



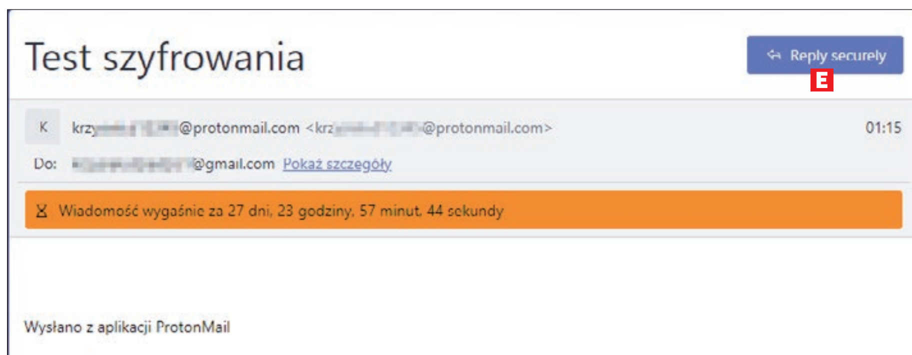
adam13zajac@gmail.com



5 Dopiero na nowej stronie w przeglądarce odbiorca będzie mógł wpisać hasło i nacisnąć **Decrypt** **D**, co pozwoli na uzyskanie dostępu do wiadomości.

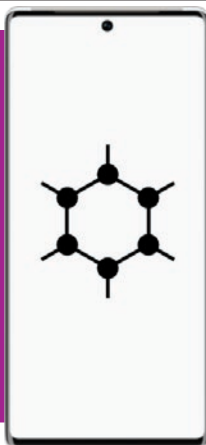


6 Co ważne, dzięki tej unikalnej opcji osoby niekorzystające na co dzień z usługi ProtonMail mogą nam odpisać, również szyfrując wiadomość – wystarczy, że skorzystają z opcji **Reply securely** **E**. Dzięki takiej formie wymiany wiadomości możemy być pewni, że nikt niepowołany nie odczyta naszych wiadomości.



ROZWIĄZANIA SYSTEMOWE

Osoby, dla których prywatność jest najważniejsza, mogą rozważyć korzystanie z alternatywnych systemów operacyjnych na smartfonach. Przykładem może być **GrapheneOS**, system open source oparty na Androidzie, kompatybilny na przykład z niektórymi modelami Google Pixel. Jest to system, który oferuje najnowsze i najlepsze rozwiązania pod względem bezpieczeństwa i prywatności.



Niektóre z jego funkcji to: tryb sandbox, nowy alokator pamięci, zabezpieczone jądro systemu, weryfikacja podczas bootowania systemu, randomizacja adresu MAC oraz wsparcie pełnej enkrypcji dysku urządzenia.

adam13zajac@gmail.com

8 Obrona smartfona przed intruzami i ochrona danych

Wiemy już z poprzedniego rozdziału, jak w bezpieczny sposób korzystać ze smartfona. Przeczytajmy teraz, jak zabezpieczyć go przed różnego rodzaju spamem, sprawdzić, czy do systemu nie przedostał się szpieg oraz jak na wszelki wypadek stworzyć kopię zapasową danych

Blokowanie spamu, połączeń i wiadomości SMS

Coraz częściej spamerzy atakują nas różnego rodzaju wiadomościami, które z jednej strony mogą być po prostu zwykłą reklamą, a z drugiej potencjalnym atakiem na naszą prywatność. Wystarczy, że naciśniemy link w SMS-ie, pobierzemy i uruchomimy niebezpieczny plik, a nasze urządzenie zostanie zainfekowane. Jest bardzo dużo rodzajów ataków, dlatego też warto wyrobić sobie nawyk, aby nie ufać wiadomościom od nieznanych nam nadawców.

PODEJRZENIE SPAMU

Połączenia przychodzące automatycznie rozpoznane jako spam są coraz częściej oznaczane wykrzyknikiem i informacją „Podejrzenie spamu". Jest to spowodowane tym, że wielu użytkowników zgłosiło dany numer jako niepożądany. Są to połączenia od telemarketerów, infolinii banków, a nawet próby wyłudzenia lub oszustwa. Takie numery możemy właściwie od razu blokować.

Po pierwsze, nie odpisujemy na żadne wiadomości, które zawierają spam, a po drugie, nie naciskamy żadnych linków.

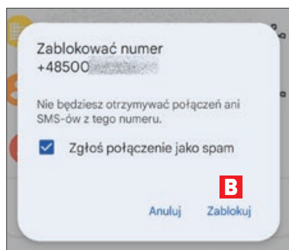
Blokujemy wybrane numery telefonu

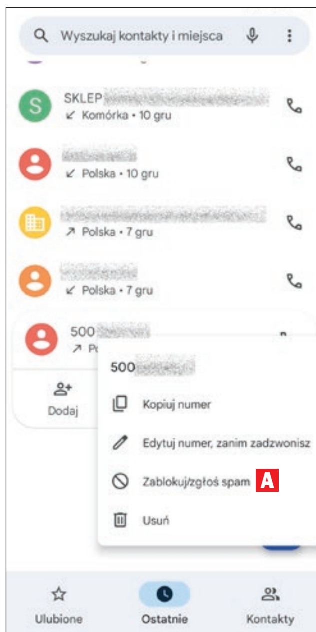
Jeśli stosunkowo rzadko zdarza się, że otrzymujemy wiadomość z podejrzaną treścią lub zwykły spam, możemy ręcznie zablokować danego nadawcę w systemie Android.

1 Otwieramy **Kontakty** na naszym urządzeniu, a następnie przytrzymujemy palec na kontakcie, który chcemy zablokować, i z menu wybieramy opcję **Zablokuj/zgłoś spam** **A**.

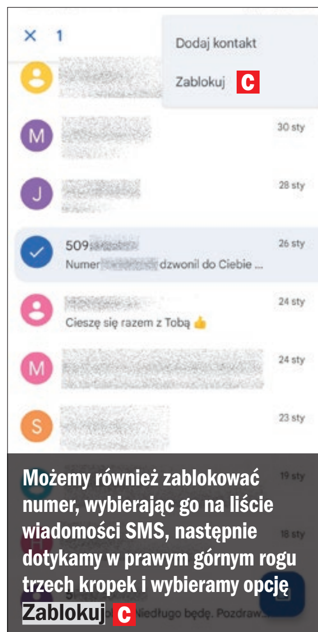
adam13zajac@gmail.com

2 Następnie, jeśli dodatkowo chcemy zgłosić podany numer jako spam, zaznaczamy odpowiednią opcję i naciskamy **Zablokuj** **B**.



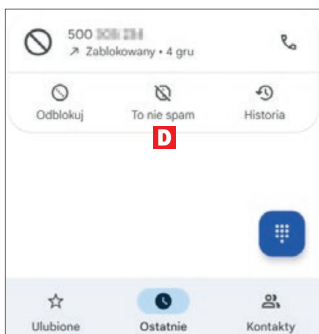


3 Od tej chwili wszelkie połączenia oraz wiadomości od tego numeru będą blokowane, a jego status będzie wyświetlany jako **Zablokowany**.



Możemy również zablokować numer, wybierając go na liście wiadomości SMS, następnie dotykamy w prawym górnym rogu trzech kropek i wybieramy opcję Zablokuj **C**

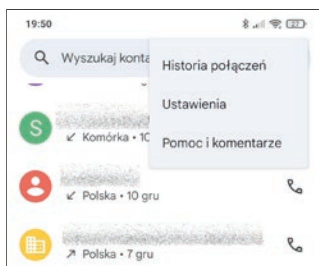
4 Kontakt możemy w każdej chwili odblokować, wystarczy go dotknąć i wybrać opcję **Odblokuj**, lub odwołać zgłoszenie go jako spamu, naciskając **To nie spam** **D**.



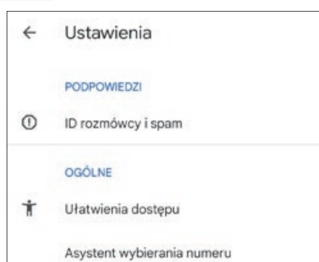
Korzystamy z filtra antyspamowego

Jeśli korzystamy z aplikacji **Telefon Google**, która ma wbudowany filtr antyspamowy, przy konkretnych numerach jest wyświetlane oznaczenie informujące o spamie. Ułatwia to blokowanie podejrzanych kontaktów. Warto aktywować tę funkcję w ustawieniach aplikacji.

1 Po uruchomieniu aplikacji **Telefon Google** naciskamy w prawym górnym rogu ikonę trzech kropek, a potem wybieramy **Ustawienia**.

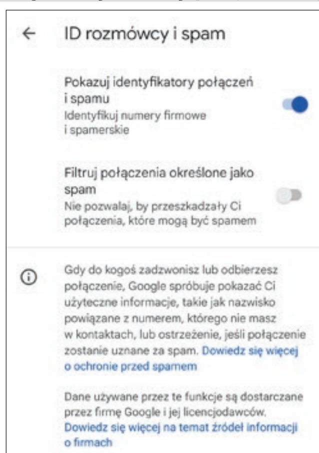


2 Następnie naciskamy **ID rozmówcy i spam**.



adam13zajac@gmail.com

3 Teraz wystarczy aktywować opcję **Pokazuj identyfikatory połączeń i spamu**.

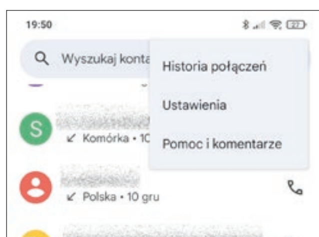


4 Jeśli chcemy, możemy również włączyć automatyczne filtrowanie połączeń sklasyfikowanych jako spam **A**. Dzięki temu podejrzane połączenia będą nie tylko oznaczane, ale od razu blokowane. Zastanówmy się jednak, zanim aktywujemy tę opcję – czasem powoduje ona automatyczne blokowanie takich połączeń jak obsługa klienta banku.

Blokujemy połączenia z nieznanych numerów

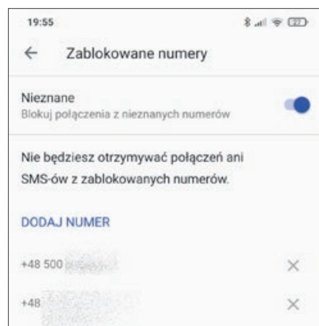
Jeśli nie chcemy otrzymywać połączeń od dzwoniących z ukrytym numerem („nieznany numer"), możemy skorzystać z opcji blokowania takich połączeń.

1 Po uruchomieniu aplikacji Telefon Google klikamy w prawym górnym rogu na symbol trzech kropek, a następnie na **Ustawienia**.



2 Następnie naciskamy **Zablokowane numery**.

3 Teraz zaznaczamy opcję **Nieznane**, aby blokować połączenia z nieznanych numerów.



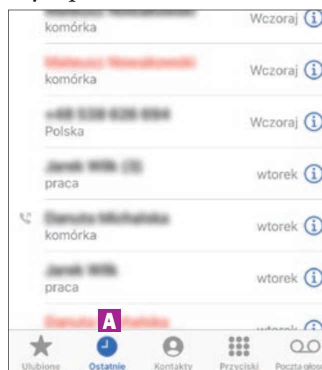
Dodatkowo w tym menu znajdziemy wszystkie zablokowane przez nas numery. Możemy je odblokować z poziomu tego widoku, naciskając **x** po prawej stronie.

Blokujemy numery telefonu na iPhonie

Blokowanie numeru telefonu jest równie proste na urządzeniach pracujących pod systemem iOS i wymaga zaledwie kilku dotknięćkliknięć.

1 Otwieramy aplikację **Telefon**.

2 Wchodzimy w zakładkę **Ostatnie** **A** na dolnym pasku.



NAGRYWANIE ROZMÓW NA SMARTFONIE

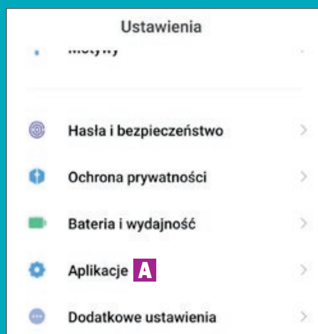
Z tym tematem wiąże się wiele kontrowersji. W przypadku urządzeń pracujących z systemem Android możliwość rejestrowania połączeń występuje praktycznie od początku. Jednak ze względu na regulacje prawne dotyczące rynku europejskiego urządzenia, które trafiają na nasz rynek, obecnie nie mają fabrycznie odblokowanych możliwości rejestrowania połączeń. Można obejść to ograniczenie, instalując specjalne aplikacje ze sklepu, na przykład **ACR** lub **Cube ACR**. Jeśli jednak mamy na naszym urządzeniu system Android w wersji 11 lub wyższej, te apki nie zadziałają.
Jakiś czas temu można było kupić urządzenia marki Huawei, które domyślnie miały dostępną systemową funkcję nagrywania połączeń, obecnie jednak trudno je dostać.
Jeśli jednak zależy nam na możliwości nagrywania połączeń, są rozwiązania, które zapewnią taką funkcjonalność. W większości przypadków wymagają rootowania telefonu w celu uzyskania praw administratora i możliwości dokonywania modyfikacji w systemie oraz instalacji dodatkowych modułów. Proces ten może się bardzo różnić w zależności od modelu urządzenia.
Należy również pamiętać o legalności nagrywania – rozmówca powinien być o tym informowany, dodatkowo musi wyrazić zgodę. Nielegalne nagrywanie rozmów jest karalne.
Warto więc zastanowić się, czy warto ryzykować utratą gwarancji na smartfon i ewentualnymi problemami prawnymi.

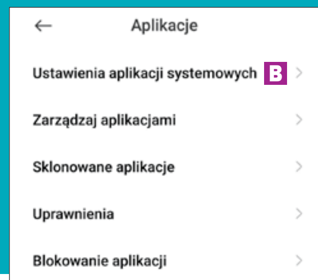
1 Jeśli jednak mamy urządzenie z systemem Android, które ma odblokowaną fabrycznie możliwość nagrywania rozmów, znajdziemy ją, klikając na **Ustawienia**, **Aplikacje** **A**.

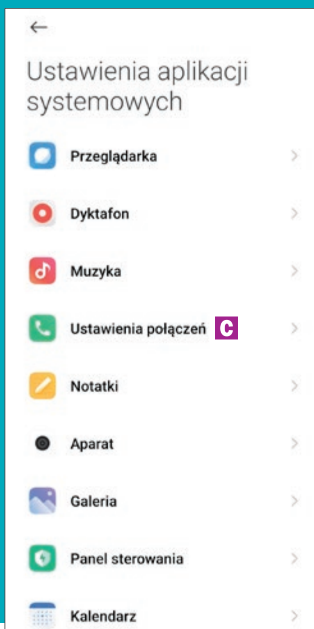
2 Następnie naciskamy **Ustawienia aplikacji systemowych** **B**.

3 Na kolejnym ekranie naciskamy **Ustawienia połączeń** **C**.

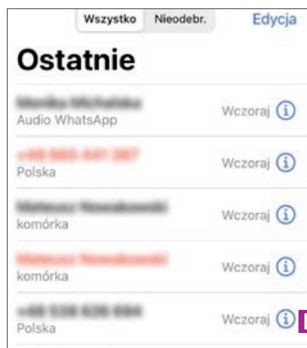
4 Teraz naciskamy **Nagrywanie połączeń** i aktywujemy funkcję nagrywania. Jeśli nie mamy dostępnej tej opcji, to oznacza, że nasze urządzenie ma fabrycznie zablokowane nagrywanie i instalowanie dodatkowych aplikacji nam nie pomoże.

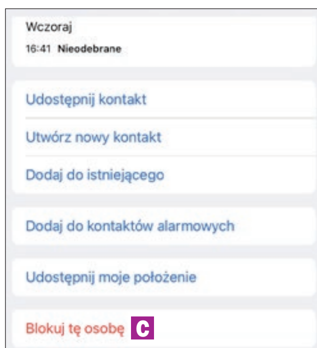


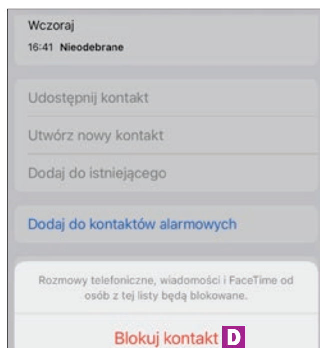




adam13zajac@gmail.com







3 Naciskamy symbol **i** **B** po prawej stronie numeru, który chcemy zablokować.

4 Wybieramy z listy opcję **Blokuj tę osobę** **C**, a potem **Blokuj kontakt** **D**.

Pegasus a nasza prywatność na smartfonie

Pegasus to opracowane przez izraelską firmę NSO Group oprogramowanie, którego głównym zadaniem jest szpiegowanie użytkowników smartfonów. Po wgraniu na smartfon ma możliwość pobrania wszystkich kontaktów, zdjęć, wiadomości oraz umożliwia podsłuchiwanie rozmów telefonicznych. Dodatkowo daje dostęp do mikrofonu i kamery urządzenia oraz przechwytuje wszelkie dane wprowadzane z klawiatury smartfona.
W trakcie śledztwa przeprowadzonego na 50 tysiącach urządzeń okazało się, że ponad tysiąc urządzeń było inwigilowanych w ponad 50 krajach i podsłuch dotyczył dziennikarzy, urzędników, polityków itp.
Infekowanie urządzeń może nastąpić na kilka sposobów. Najczęstszym mechanizmem jest wysłanie wiadomości – SMS, iMessage lub Google Czat – z niebezpiecznym linkiem. Po odczytaniu tej wiadomości i naciśnięciu linku ofiara jest infekowana poprzez wykorzystanie luk bezpieczeństwa zero-day (błędów w oprogramowaniu nienaprawionych jeszcze przez producentów). Według ostatnich badań szczególnie narażeni mogą być użytkownicy urządzeń firmy Apple, którzy korzystają z wiadomości iMessage. Poprzez wykrytą ostatnio lukę zero-click atakujący może zainfekować iPhone, jedynie wysyłając wiadomość – po jej odczytaniu użytkownik zostaje zainfekowany, nie jest wymagane żadne jego działanie.

Sprawdzamy, czy jesteśmy zainfekowani

Twórcy oprogramowania szpiegowskiego starają się jak najlepiej ukryć swoje aplikacje – tak aby były nie do wykrycia.
Eksperci od bezpieczeństwa natomiast starają się tworzyć narzędzia, które pozwalają na wykrywanie mechanizmów śledzenia.
W przypadku smartfona najbardziej polecanym sposobem sprawdzania, czy został on zaatakowany i jest lub mógł być szpiegowany, jest skorzystanie z oprogramowania **Mobile Verification Toolkit** (**MVT**) przygotowanego przez **Amnesty International**.
Narzędzie to bada pliki konfiguracyjne urządzenia. Nie wskazuje jednak jednoznacznie, czy doszło do ataku, a jedynie informuje o wykryciu wskaźników, które mogą sugerować włamanie – należy o tym pamiętać.

adam13zajac@gmail.com

KORZYSTAMY Z MOBILE VERIFICATION TOOLKIT

MVT to narzędzie stworzone przez Amnesty International. Stosowanie go nie jest, niestety, najprostsze, dlatego też zaleca się korzystanie z niego nieco bardziej doświadczonym użytkownikom.
MVT to tak naprawdę cały zbiór narzędzi zaprojektowanych w celu zidentyfikowania wszelkich oznak włamania do urządzenia mobilnego (iOS i Android) . Najważniejsze funkcje MVT to:

- Odszyfrowanie kopii zapasowych iOS;
- Analiza rekordów z wielu baz danych dla systemu iOS, aplikacji, dzienników systemu i innych;
- Wyodrębnianie aplikacji z urządzeń z systemem Android;
- Wyodrębnianie danych diagnostycznych;
- Generowanie dzienników JSON;
- Generowanie chronologicznej osi czasu z wyodrębnionymi rekordami w celu wykrycia śladów szkodliwego oprogramowania.

Zanim zaczniemy korzystać z MVT, należy wiedzieć, że wymaga on do działania **Pythona** w wersji 3.6+. Dodatkowo korzystanie z oprogramowania w środowisku Windows nie jest wspierane i pomimo że narzędzie może zadziałać, mogą pojawić się różnego typu błędy. Zalecanym środowiskiem jest Linux.
Ze względu jednak na to, że większość czytelników korzysta z Windows, w naszym przykładzie pokazano, jak przebiega cały proces pod Windows i Androidem. Jeśli jednak pojawią się problemy, należy uruchomić to oprogramowania pod Linuxem.

1 Po poprawnym zainstalowaniu środowiska Python w wersji 3.6+ i dodaniu wszelkich zmiennych środowiskowych do PATH uruchamiamy Wiersz polecenia jako administrator i wpisujemy polecenie **pip3 install mvt** **A**.

```
C:\WINDOWS\system32>pip3 install mvt   A
Collecting mvt
  Downloading mvt-1.5.1-py3-none-any.whl (352 kB)
     |████████████████████████████████| 352 kB 3.3 MB/s
Collecting libusb1>=2.0.1
  Downloading libusb1-3.0.0-py3-none-win_amd64.whl (140 kB)
     |████████████████████████████████| 140 kB 3.3 MB/s
Requirement already satisfied: packaging>=21.0 in c:\users\krzys\app
) (21.3)
Collecting requests>=2.26.0
  Downloading requests-2.27.1-py2.py3-none-any.whl (63 kB)
     |████████████████████████████████| 63 kB 2.3 MB/s
Collecting simplejson>=3.17.5
  Downloading simplejson-3.17.6-cp39-cp39-win_amd64.whl (75 kB)
     |████████████████████████████████| 75 kB 2.6 MB/s
Collecting iOSbackup>=0.9.921
  Downloading iOSbackup-0.9.921-py3-none-any.whl (18 kB)
```

2 Rozpocznie się instalacja całego pakietu wraz z wszystkimi niezbędnymi dodatkami. Po zainstalowaniu będziemy mieli pełny dostęp do narzędzi **mvt-ios** oraz **mvt-android**, każde z nich służy do analizy urządzeń z odpowiednim systemem operacyjnym.

3 Następnie musimy zainstalować **Android Debug Bridge (adb)**, jest to narzędzie wchodzące w skład **Android SDK** – opis instalacji znajduje się na stronie 98.

4 Po podłączeniu urządzenia w trybie debugowania w Wierszu polecenia wykonujemy komendę **mvt-android check-adb --output C:/test**. Jeśli pojawi się błąd, jak w przykładzie **B**, należy wykonać komendę **adb kill-server** i ponownie spróbować.

```
C:\WINDOWS\system32>mvt-android check-adb --output C:/test


        MVT - Mobile Verification Toolkit
                https://mvt.re
                Version: 1.5.1


12:24:01 INFO     [mvt.android.cli] Checking Android through adb bridge
         INFO     [mvt.android.cli] Loaded a total of 0 unique indicators
         INFO     [mvt.android.modules.adb.chrome_history] Running module ChromeHistory...
    B    CRITICAL [mvt.android.modules.adb.base] Device is busy, maybe run `adb kill-server` and try again.

C:\WINDOWS\system32>_
```

>

adam13zajac@gmail.com


```
C:\WINDOWS\system32>mvt-android check-adb --output C:/test   C

        MVT - Mobile Verification Toolkit
                https://mvt.re
                Version: 1.5.1

12:27:47 INFO     [mvt.android.cli] Checking Android through adb bridge
         INFO     [mvt.android.cli] Loaded a total of 0 unique indicators
         INFO     [mvt.android.modules.adb.chrome_history] Running module ChromeHistory...
         ERROR    [mvt.android.modules.adb.chrome_history] This module is optionally available in case the device is
                  already rooted. Do NOT root your own device!
         INFO     [mvt.android.modules.adb.sms] Running module SMS...
         INFO     [mvt.android.modules.adb.sms] Insufficient privileges for module SMS: This module is optionally
                  available in case the device is already rooted. Do NOT root your own device!
         INFO     [mvt.android.modules.adb.whatsapp] Running module Whatsapp...
         ERROR    [mvt.android.modules.adb.whatsapp] This module is optionally available in case the device is already
                  rooted. Do NOT root your own device!
         INFO     [mvt.android.modules.adb.processes] Running module Processes...
12:27:48 INFO     [mvt.android.modules.adb.processes] Extracted records on a total of 625 processes
         INFO     [mvt.android.modules.adb.getprop] Running module Getprop...
         INFO     [mvt.android.modules.adb.getprop] Extracted 1057 Android system properties
         INFO     [mvt.android.modules.adb.getprop] The Getprop module does not support checking for indicators
         INFO     [mvt.android.modules.adb.settings] Running module Settings...
         WARNING  [mvt.android.modules.adb.settings] Found suspicious setting "install_non_market_apps = 1" (enabled
                  installation of non-market apps)
         INFO     [mvt.android.modules.adb.selinux_status] Running module SELinuxStatus...
```

```
 no.mobitroll.kahoot.android  D       | /data/app/no.mobitroll.kahoot.android-IW… | no | no | 0
 net.metaquotes.metatrader5           | /data/app/net.metaquotes.metatrader5-qOC… | no | no | 0
 com.riteshsahu.SMSBackupRestore      | /data/app/com.riteshsahu.SMSBackupRestor… | no | no | 0
 com.google.earth                     | /data/app/com.google.earth-rScT5p5m5Aqfk… | no | no | 0
 cn.wps.moffice_eng                   | /data/app/cn.wps.moffice_eng-oubJBbgPFKT… | no | no | 0
 cn.wps.moffice_eng                   | /data/app/cn.wps.moffice_eng-oubJBbgPFKT… | no | no | 0
 com.microsoft.teams                  | /data/app/com.microsoft.teams-Dr_xvD3r2W… | no | no | 0

12:33:53 INFO     [mvt.android.modules.adb.packages] Extracted at total of 467 installed package names
         INFO     [mvt.android.modules.adb.logcat] Running module Logcat...
12:33:54 INFO     [mvt.android.modules.adb.logcat] Current logcat logs stored at C:/test\logcat.txt
         INFO     [mvt.android.modules.adb.logcat] Logcat logs prior to last reboot stored at C:/test\logcat_last.txt
         INFO     [mvt.android.modules.adb.logcat] The Logcat module does not support checking for indicators
         INFO     [mvt.android.modules.adb.root_binaries] Running module RootBinaries...
12:33:55 INFO     [mvt.android.modules.adb.root_binaries] The RootBinaries module does not support checking for
                  indicators
         INFO     [mvt.android.modules.adb.files] Running module Files...
12:33:57 INFO     [mvt.android.modules.adb.files] Found 30243 files in primary Android data directories
         INFO     [mvt.android.modules.adb.files] Processing full file listing. This may take a while...
12:34:10 INFO     [mvt.android.modules.adb.files] Found 379879 total files

C:\WINDOWS\system32>
```

5 Po poprawnym uruchomieniu narzędzia rozpocznie się sprawdzanie naszego urządzenia. Pełna analiza będzie dostępna w pliku wyjściowym, który będzie się znajdować na dysku **C** w folderze **test** **C**.

6 W trakcie pracy narzędzia zostaną przeanalizowane wszystkie nasze aplikacje **D** – cały proces może trwać dość długo.

7 Teraz wykonujemy polecenie **mvt-android download-iocs** **E** w celu pobrania plików ze znacznikami narzędzi szpiegowskich, w tym Pegasusa.

8 Pliki te domyślnie po pobraniu znajdują się w lokalizacji: **C:\Users\krzys\AppData\Local\mvt\mvt** **F** – gdzie **krzys** to nazwa naszego zalogowanego w Windows użytkownika.

9 Wykonujemy komendę **mvt-android check-iocs --iocs [lokalizacja pliku z rozszerzeniem STIX2] C:\test** **G**

```
C:\WINDOWS\system32>mvt-android download-iocs   E

        MVT - Mobile Verification Toolkit
                https://mvt.re
                Version: 1.5.1

12:44:32 INFO     [mvt.android.cli] Downloading indicator file NSO Group Pegasus Indicators of Compromise from
                  https://raw.githubusercontent.com/AmnestyTech/investigations/master/2021-07-18_nso/pegasus.stix2
         INFO     [mvt.android.cli] Saved indicator file to
                  raw.githubusercontent.com_AmnestyTech_investigations_master_2021-07-18_nso_pegasus.stix2
         INFO     [mvt.android.cli] Downloading indicator file Cytrox Predator Spyware Indicators of Compromise from
                  https://raw.githubusercontent.com/AmnestyTech/investigations/master/2021-12-16_cytrox/cytrox.stix2
         INFO     [mvt.android.cli] Saved indicator file to
                  raw.githubusercontent.com_AmnestyTech_investigations_master_2021-12-16_cytrox_cytrox.stix2

C:\WINDOWS\system32>_
```

› Dysk lokalny (C:) › Użytkownicy › krzys › AppData › Local › mvt › mvt **F**

Nazwa	Data modyfikacji	Typ	Rozmiar
raw.githubusercontent.com_AmnestyTec...	17.02.2022 12:44	Plik STIX2	1 085 KB
raw.githubusercontent.com_AmnestyTec...	17.02.2022 12:44	Plik STIX2	336 KB

```
C:\WINDOWS\system32>mvt-android check-iocs --iocs C:\Users\krzys\AppData\Local\mvt\mvt\raw.githubusercontent.com_AmnestyTech_investigations_master_2021-07-18_nso_pegasus.stix2 C:\test
```
G

```
        MVT - Mobile Verification Toolkit
                https://mvt.re
                Version: 1.5.1

12:55:29 INFO     [mvt.android.cli] Checking stored results against provided indicators...
         INFO     [mvt.android.cli] Parsing STIX2 indicators file at path C:\Users\krzys\AppData\Local\mvt\mvt\raw.gith
                  ubusercontent.com_AmnestyTech_investigations_master_2021-07-18_nso_pegasus.stix2
         INFO     [mvt.android.cli] Extracted 1511 indicators for collection with name "Pegasus"
         INFO     [mvt.android.cli] Parsing STIX2 indicators file at path C:\Users\krzys\AppData\Local\mvt\mvt\raw.gith
                  ubusercontent.com_AmnestyTech_investigations_master_2021-07-18_nso_pegasus.stix2
```

w celu sprawdzenia danych zapisanych z naszego urządzenia pod kątem śladów Pegasusa.

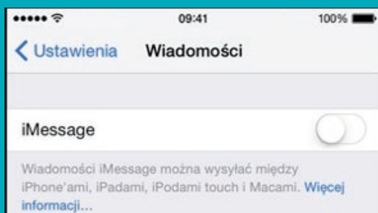
10 Jeżeli przy jakiejś pozycji pojawi się czerwony znacznik **Warning** **H**, może on wskazywać na podejrzaną aktywność na naszym urządzeniu.

Podobnie wygląda proces weryfikacji urządzeń z iOS – kompletną instrukcję można znaleźć na stronie **https://docs.mvt.re/en/latest/ios/methodology**

```
         INFO     [mvt.android.cli] Loading results from "files.json" with module Files
12:55:30 INFO     [mvt.android.modules.adb.files] Loaded 379879 results from "C:\test\files.json"
12:55:32 INFO     [mvt.android.cli] Loading results from "getprop.json" with module Getprop
         INFO     [mvt.android.modules.adb.getprop] Loaded 1057 results from "C:\test\getprop.json"
         INFO     [mvt.android.cli] Loading results from "packages.json" with module Packages
         INFO     [mvt.android.modules.adb.packages] Loaded 467 results from "C:\test\packages.json"
         INFO     [mvt.android.cli] Loading results from "processes.json" with module Processes
         INFO     [mvt.android.modules.adb.processes] Loaded 625 results from "C:\test\processes.json"
         INFO     [mvt.android.cli] Loading results from "selinux_status.json" with module SELinuxStatus
         INFO     [mvt.android.modules.adb.selinux_status] Loaded 1 results from "C:\test\selinux_status.json"
         INFO     [mvt.android.cli] Loading results from "settings.json" with module Settings
         INFO     [mvt.android.modules.adb.settings] Loaded 3 results from "C:\test\settings.json"
       H WARNING  [mvt.android.modules.adb.settings] Found suspicious setting "install_non_market_apps = 1" (enabled
                  installation of non-market apps)
```

BLOKUJEMY FUNKCJĘ iMESSAGE

Jeśli boimy się zainfekowania Pegasusem lub innych ataków z wykorzystaniem luk zero-click (niewymagających żadnych działań użytkownika) na urządzeniach z systemem iOS korzystających z funkcjonalności iMessage, możemy ją po prostu wyłączyć – wtedy będziemy korzystać ze zwykłych SMS-ów/MMS-ów, w wypadku których do zainfekowania konieczne jest naciśnięcie linku przez użytkownika (jeżeli nie będziemy naciskać, będziemy bezpieczni).



1 Otwieramy **Ustawienia**. Następnie naciskamy opcję **Wiadomości**.

2 Teraz wyłączamy opcję iMessage.

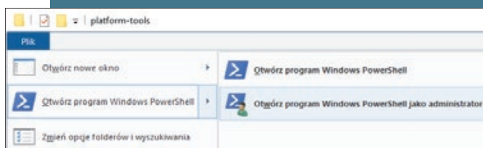
DLA ZAAWANSOWANYCH

ADB W WINDOWS – INSTALACJA I KORZYSTANIE

ADB to zestaw narzędzi, który umożliwia deweloperom szybki dostęp do urządzeń z systemem Android. Pozwala na wykonywanie zaawansowanych operacji, jak tworzenie kopii zapasowych, diagnostyka, instalacja aplikacji. Nawiązywanie połączeń z wykorzystaniem ADB jest konieczne przy zaawansowanych operacjach na urządzeniu i wymaga większego doświadczenia.

1 Pobieramy paczkę ZIP z oficjalnej strony Google: **https://dl.google.com/android/repository/platform-tools-latest-windows.zip**

2 Po wypakowaniu wchodzimy do nowego folderu i klikamy w górnym lewym rogu na **Plik**, **Otwórz program Windows PowerShell jako administrator**.



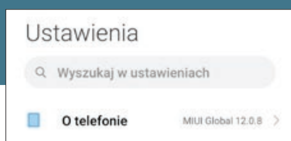
3 Wpisujemy komendę **./adb devices** i zatwierdzamy klawiszem [enter]. Służy ona do wylistowania wszystkich urządzeń z systemem Android podłączonych do komputera. Jeśli pojawi się napis **daemon started successfully**, możemy przejść do konfiguracji na smartfonie.

Administrator: Windows PowerShell

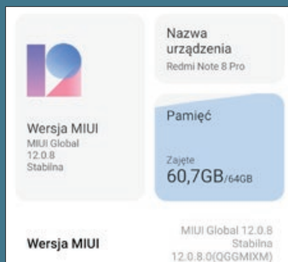
```
PS D:\platform-tools> ./adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully
List of devices attached

PS D:\platform-tools> _
```

4 Na naszym smartfonie otwieramy **Ustawienia**, następnie przechodzimy do **O telefonie**.



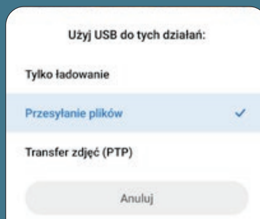
5 Teraz siedem razy naciskamy numer wersji (wersja MIUI lub inna nazwa z oprogramowaniem) w celu odblokowania **Opcji programistycznych**.

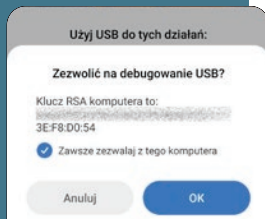


6 Teraz w opcjach programistycznych włączymy funkcję **Debugowanie USB**. **Uwaga!** Gdy już nie będziemy potrzebować tej funkcji, należy ją ponownie zablokować, gdyż może sprawić, że urządzenie będzie bardziej podatne na ataki.



7 Teraz podłączamy nasze urządzenie do komputera przewodem USB. Wybieramy opcję **Przesyłanie plików**, wyrażamy zgodę na debugowanie USB i ponownie wykonujemy polecenie **./adb devices**.





8 Jeśli wszystko wykonaliśmy poprawnie, pojawi się wpis z wykrytym jednym urządzeniem. Teraz możemy wykonywać wiele bardziej zaawansowanych wskazówek.

```
PS D:\platform-tools> ./adb devices
List of devices attached
5lknw8heeahay58p        device

PS D:\platform-tools>
```

adam13zajac@gmail.com

CO TO JEST ADB

Android Debug Bridge lub w skrócie **ADB** to interfejs służący do komunikacji i zarządzania urządzeniem z systemem Android z poziomu komputera. Google udostępniło w pakiecie dla deweloperów interfejs ADB, który pozwala na testowanie urządzeń z systemem Android, wprowadzanie modyfikacji, testowanie aplikacji, tworzenie zrzutów pamięci i wielu różnych zadań, których nie daje się wykonać z poziomu samego smartfona bądź też oprogramowania producentów urządzeń. Zwykli użytkownicy, korzystając z ADB, mogą: kopiować pliki z urządzenia, przesyłać pliki do urządzenia, instalować i usuwać aplikacje, wykonywać kopie zapasowe i je przywracać, tworzyć zrzuty logów i wiele, wiele więcej.
Dodatkowo do korzystania z tego narzędzia nie musimy mieć uprawnień administratora (roota), więc opisywane na tych stronach porady sprawdzą się w przypadku wszystkich urządzeń z systemem Android.

ADB: kopia zapasowa i analiza, co się dzieje

Wykonujemy pełną kopię zapasową

W przypadku interfejsu ADB nie jest wymagane posiadanie roota. Ta wskazówka jest dość uniwersalna. Powinna zadziałać w przypadku każdego urządzenia niezależnie od wersji systemu Android. Tak utworzona kopia pozwala na zachowanie nie tylko aplikacji, ale również ich ustawień. Jedynym minusem jest to, że może być ona odtworzona tylko i wyłącznie na tym samym modelu urządzenia, na jakim została wykonana.
Uwaga! Pamiętajmy, że do korzystania z możliwości ADB musimy aktywować tryb debugowania na naszym urządzeniu. Pamiętajmy również, aby go dezaktywować, gdy nie będziemy już z niego korzystać (patrz strona 98).

1 Podłączamy telefon poprzez USB, uruchamiamy Wiersz polecenia w folderze, w którym umieściliśmy ADB, i wykonujemy komendę **adb devices**.

```
Administrator: Wiersz polecenia

D:\platform-tools>adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully
List of devices attached
51knw8heeahay58p        device

D:\platform-tools>
```

2 Po zweryfikowaniu poprawnego połączenia wykonujemy polecenie **adb backup -all** w celu wykonania kopii wszystkich aplikacji i danych.

```
D:\platform-tools>adb backup -all
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

3 Na ekranie smartfona pojawi się informacja o wykonywaniu kopii, którą należy zatwierdzić, naciskając **Utwórz kopię zapasową danych**. Dla bezpieczeństwa możemy zaszyfrować kopię, podając hasło.

Pełna kopia zapasowa

Zażądano wykonania pełnej kopii zapasowej wszystkich danych na podłączonym komputerze stacjonarnym. Czy chcesz na to zezwolić?

Jeśli żądanie utworzenia kopii zapasowej nie pochodzi od Ciebie, nie zezwalaj na kontynuowanie tej operacji.

Jeśli chcesz zaszyfrować pełną kopię zapasową, wprowadź poniżej hasło:

NIE TWÓRZ KOPII ZAPASOWEJ | UTWÓRZ KOPIĘ ZAPASOWĄ DANYCH

NAJCZĘŚCIEJ WYKORZYSTYWANE POLECENIA – SZYBKA ŚCIĄGA

Jeśli zamierzamy efektywnie korzystać z interfejsu **ADB**, warto znać popularne komendy. Dzięki temu wiele zadań wykonamy bardzo szybko. Zdecydowaną większość komend poprzedzamy przedrostkiem **adb** – chyba że została dokładnie podana komenda innego typu.

- **devices** – wyświetlanie listy podłączonych urządzeń
- **push** – służy do przesyłania plików z komputera na urządzenia z systemem Android
- **pull** – służy do pobierania plików z urządzenia z systemem Android na komputer
- **install** – umożliwia instalowanie aplikacji
- **uninstall** – pozwala usuwać aplikacje z urządzenia
- **shell** – służy do uzyskania dostępu do powłoki urządzenia i wydawania kolejnych komend
- **kill-server** – umożliwia zresetowanie interfejsu ADB
- **backup** – służy do wykonywania kopii zapasowej urządzenia
- **restore** – umożliwia odtwarzanie kopii zapasowej
- **reboot** – pozwala na ponowne uruchomienie urządzenia z poziomu komputera.

Uwaga! Od wersji Android 11 Google podjęło decyzję o ograniczeniu możliwości komendy **adb backup**. Wcześniej skorzystanie z niej pozwalało wykonać pełną kopię wraz ze wszystkimi ustawieniami i danymi. Obecnie możemy wykonać kopię aplikacji, lecz jeśli ma ona ustawione określone flagi, nie będziemy mogli zapisać całej jej konfiguracji.

```
D:\platform-tools>adb shell dumpsys battery
adb server version (36) doesn't match this client (41); killing...
* daemon started successfully
Current Battery Service state:
  AC powered: false
  USB powered: true
  Wireless powered: false
  Max charging current: 500000
  Max charging voltage: 5000000
  Charge counter: 2946000
  status: 2
  health: 2
  present: true
  level: 100
  scale: 100
  voltage: 4158
  temperature: 300
  technology: Li-poly

D:\platform-tools>_
```

A

Przywracamy dane z kopii zapasowej

1 W celu przywrócenia danych z kopii zapasowej wykonujemy krok pierwszy z ostatniej porady.

2 Następnie wykonujemy polecenie **adb restore backup.ab**, gdzie backup.ab to domyślna nazwa utworzonej w poprzedniej wskazówce kopii zapasowej. Na naszym urządzeniu potwierdzamy chęć przywrócenia danych i czekamy na zakończenie całego procesu.

```
D:\platform-tools>adb restore backup.ab_
```

Poznajemy dane dotyczące podzespołów systemu

Dzięki integracji interfejsu **adb** z powłoką interaktywną systemu Android możemy poznać szczegółowe informacje na temat całego systemu i różnych podzespołów, w tym na przykład baterii.

adam13zajac@gmail.com

1 Po podłączeniu urządzenia do komputera i zweryfikowaniu połączenia wykonujemy polecenie: **adb shell dumpsys battery** **A**.

2 Możemy od razu sprawdzić, jaką metodą ładowane jest nasze urządzenie i czy w ogóle jest ładowane.

3 Oczywiście, wpisując polecenie **adb shell dumpsys**, otrzymamy zrzut informacji o wszystkich modułach naszego urządzenia. **Warto wiedzieć:** Pełna analiza zrzutu systemu może być podstawą do analizy problemów z urządzeniem.

Korzystamy z powłoki shell w celu weryfikacji procesów i aplikacji

Polecenie **shell** pozwala na tworzenie interaktywnej powłoki i wykonywanie komend bezpośrednio w systemie Android, tak jak ma to miejsce w systemach Linux. Możemy wykonywać znacznie więcej poleceń znanych ze świata Linuxa.

1 Po podłączeniu urządzenia do komputera i zweryfikowaniu połączenia wykonujemy polecenie: **adb shell** – powinniśmy zobaczyć podobny widok:

```
Administrator: Wiersz polecenia - adb shell
D:\platform-tools>adb shell
begonia:/ $
```

2 Teraz możemy wpisywać dowolne polecenie, na przykład **cat /proc/cpuinfo**, w celu poznania modelu procesora.

```
Administrator: Wiersz polecenia - adb shell
rocessor        : 7
ogoMIPS         : 26.00
eatures         : fp asimd evtstrm
PU implementer  : 0x41
PU architecture: 8
PU variant      : 0x3
PU part         : 0xd0b
PU revision     : 0

ardware         : MT6785V/CC
egonia:/ $
```

UKRYTA FUNKCJA NAGRYWANIA EKRANU

ADB pozwala również na tworzenie nagrania z ekranu naszego urządzenia mobilnego. Dzięki temu będziemy mogli nagrywać na przykład filmy instruktażowe lub pokazać komuś, jaki mamy problem na naszym urządzeniu bez potrzeby instalowania oprogramowania do współdzielenia pulpitu. Pokażemy na nagraniu jedynie to, co chcemy.

```
Administrator: Wiersz polecenia
:\platform-tools>adb shell screenrecord --time-limit 10 /sdcard/mojeNagranie.mp4
```

A

```
Administrator: Wiersz polecenia
:\platform-tools>adb pull /sdcard/mojeNagranie.mp4
/sdcard/mojeNagranie.mp4: 1 file pulled, 0 skipped. 15.4 MB/s (16616501 bytes in 1.032s)

:\platform-tools>
```

B


C

1 Po podłączeniu urządzenia do komputera i zweryfikowaniu połączenia wykonujemy polecenie: **adb shell screenrecord --time-limit 10 /sdcard/mojeNagranie.mp4** **A**. Zapis **--time-limit 10** pozwala określić, jak długie ma być nagranie, gdzie 10 to liczba sekund.

2 Możemy od razu pobrać plik na nasz komputer, korzystając z polecenia **pull: adb pull /sdcard/mojeNagranie.mp4** **B**. Nagranie **C** jest domyślnie zapisywane w wysokiej jakości z rozdzielczością domyślną dla naszego urządzenia.

adam13zajac@gmail.com


```
Administrator: Wiersz polecenia - adb shell
Tasks: 614 total,   2 running, 612 sleeping,   0 stopped,   0 zombie
  Mem:      5.3G total,      5.2G used,     171M free,      70M buffers
 Swap:      2.9G total,      2.2G used,     678M free,     1.8G cached
800%cpu   7%user   0%nice  17%sys 769%idle   7%iow   0%irq   0%sirq   0%host
  PID USER         PR  NI VIRT  RES  SHR S[%CPU] %MEM     TIME+ ARGS
31036 shell        20   0  35M 4.3M 3.2M R 17.2   0.0   0:00.04 top B
  745 system       20   0  93M 2.9M 2.5M S  6.8   0.0 149:37.37 android.hardware.sensors@1.0-service-mediatek
31037 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/3:2]
31013 shell        20   0  33M 3.1M 2.6M S  0.0   0.0   0:00.02 sh
31010 root         20   0    0    0    0 I  0.0   0.0   0:00.01 [kworker/6:1]
31008 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/5:1]
30921 u0_a44       20   0 5.3G 122M  95M S  0.0   2.2   0:00.54 com.google.android.apps.turbo:aab
30917 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/2:0]
30842 root         20   0    0    0    0 I  0.0   0.0   0:00.01 [kworker/7:2]
30823 u0_a16       20   0 5.5G 108M  78M S  0.0   1.9   0:00.96 com.google.android.apps.wellbeing
30822 root         20   0    0    0    0 D  0.0   0.0   0:00.00 [kworker/3:1]
30818 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/1:0]
30817 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/4:0]
30785 root          0 -20    0    0    0 I  0.0   0.0   0:00.00 [kbase_event]
30762 u0_i0        20   0 1.9G 109M  90M S  0.0   1.9   0:00.70 com.android.chrome:sandboxed_process0:org.chromium.cont+
30732 u0_a84       20   0 1.8G  55M  44M S  0.0   1.0   0:00.19 com.android.chrome_zygote
30725 u0_a84       20   0 1.7G 114M  98M S  0.0   2.0   0:00.75 com.android.chrome:privileged_process2
30535 u0_a77       20   0 6.9G 208M 157M S  0.0   3.7   0:03.16 com.google.android.youtube
30515 u0_a28       20   0 5.5G 156M 120M S  0.0   2.8   0:00.85 com.google.android.dialer
30512 root         20   0    0    0    0 I  0.0   0.0   0:00.00 [kworker/0:0]
30163 u0_a294      20   0 5.1G 102M  76M S  0.0   1.8   0:00.41 com.xiaomi.bsp.gps.nps
29762 u0_a131      20   0 6.4G 221M 175M S  0.0   4.0   0:05.53 com.google.android.gm
29418 root          0 -20    0    0    0 I  0.0   0.0   0:00.00 [kbase_event]
29363 u0_a72       20   0 6.4G 232M 177M S  0.0   4.2   0:03.22 com.google.android.apps.maps
28962 u0_a198      16  -4 6.2G 270M 204M S  0.0   4.9   0:12.47 com.microsoft.office.outlook
```

3 Komenda **top** **B** pozwala na poznanie aktywnych procesów wraz z ich czasem uruchomienia oraz wykorzystywanymi aktualnie zasobami. Jest to bardzo przydatne, jeśli podejrzewamy, że na naszym urządzeniu jest aktywna aplikacja lub proces szpiegujący. Od razu dowiemy się również, ile dokładnie pamięci RAM wykorzystuje nasze urządzenie.

Warto wiedzieć: top to program działający z poziomu konsoli, występujący w większości uniksopochodnych systemów operacyjnych wyświetlający odświeżaną listę procesów aktualnie działających w systemie. Dzięki niemu możemy monitorować to, co aktualnie dzieje się w systemie. Dane te mogą być sortowane według różnych kryteriów, na przykład według zużywanej mocy obliczeniowej czy pamięci operacyjnej (wybór poprzez podanie odpowiedniego parametru programu). Wyświetlane są także inne dane, na przykład nazwa użytkownika, który uruchomił ten proces.

4 Wykonując polecenie **pm list packages**, uzyskamy listę wszystkich zainstalowanych w systemie pakietów i aplikacji – w ten sposób możemy namierzyć niechciane apki.

Warto wiedzieć: pm to narzędzie **Package Manager**, służy do wykonywania akcji i zapytań na wszystkich aplikacjach w systemie. Korzystając z niego możemy na przykład wyświetlić listę wszystkich aplikacji czy zainstalować lub odinstalować wybraną aplikację.

```
Administrator: Wiersz polecenia - adb shell
package:com.xtb.xmobile2
package:com.xiaomi.smarthome
package:com.lbe.security.miui
package:com.google.android.play.games
package:com.google.android.apps.adm
package:com.android.bluetooth
package:com.miui.newmidrive
package:com.examobile.bubblelevel
package:com.android.providers.contacts
package:pl.inpost.inmobile
package:no.mobitroll.kahoot.android
package:com.android.captiveportallogin
package:com.android.theme.icon.roundedrect
package:net.metaquotes.metatrader5
package:com.riteshsahu.SMSBackupRestore
package:com.android.internal.systemui.navbar.gestural_narrow_back
package:com.google.earth
package:com.android.theme.icon_pack.rounded.settings
```

adam13zajac@gmail.com

KORZYSTAMY Z ADB PRZEZ WI-FI

Domyślnie ADB korzysta z połączenia USB do interakcji z naszym urządzeniem. Możemy jednak skonfigurować możliwość łączenia bezprzewodowego, co jest bardzo przydatne – zwłaszcza jeśli planujemy częściej korzystać z tego interfejsu.

1 Łączymy się z tą samą siecią zarówno na komputerze, jak i na urządzeniu z Androidem. **Uwaga!** Nie wszystkie routery są kompatybilne; niektóre mogą domyślnie blokować próby połączeń.

2 Podłączamy urządzenie do komputera przez USB i weryfikujemy poleceniem **adb devices**, czy zostało rozpoznane.

3 Następnie konfigurujemy port nasłuchujący w naszym urządzeniu, tak abyśmy mogli nawiązać zdalne połączenie – **adb tcpip 5555**.

```
Administrator: Wiersz polecenia

D:\platform-tools>adb tcpip 5555

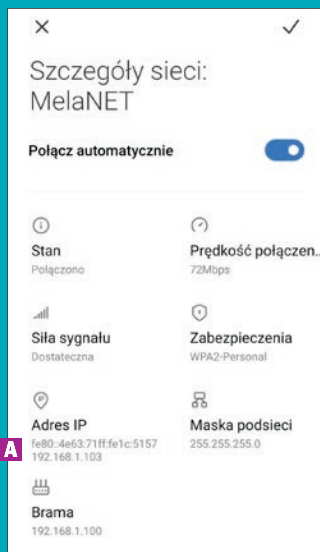
D:\platform-tools>
```

4 Odłączamy przewód USB od naszego urządzenia i odnajdujemy aktualny adres IP. Otwieramy **Ustawienia**, **Wi-Fi** i przechodzimy do szczegółów aktualnego połączenia – nasz adres IP to na przykład **192.168.1.103** **A**.

5 Na komputerze wykonujemy polecenie **adb connect adres_IP_urządzenia:port**. Po nawiązaniu połączenia możemy zweryfikować je, wykonując komendę **adb devices** (przykład: **adb connect 192.168.1.103:5555**)

```
D:\platform-tools>adb connect 192.168.1.103:5555
```

6 Od teraz możemy zdalnie korzystać z interfejsu **adb** na naszym urządzeniu – jako potwierdzenie podajemy zrzut danych na temat baterii; jak widać, nie




```
D:\platform-tools>adb devices
List of devices attached
192.168.1.103:5555      device


D:\platform-tools>_
```

jest ona w żaden sposób ładowana, czyli nie mamy połączenia przewodowego.

```
Administrator: Wiersz polecenia

):\platform-tools>adb devices
.ist of devices attached
.92.168.1.103:5555      device


):\platform-tools>adb shell dumpsys battery
urrent Battery Service state:
  AC powered: false
  USB powered: false
  Wireless powered: false
  Max charging current: 0
  Max charging voltage: 0
  Charge counter: 2946000
  status: 3
```

adam13zajac@gmail.com

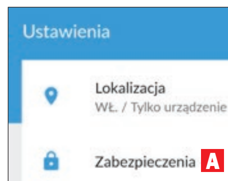
Szyfrowanie smartfona z Androidem

UWAGA!
W różnych wersjach Androida szyfrowanie może wyglądać inaczej.

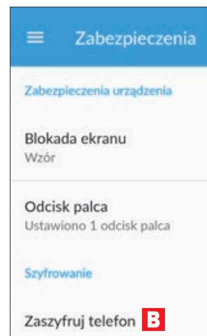
Dbając o bezpieczeństwo i prywatność, skupiamy się głównie na naszych komputerach i laptopach. Warto jednak pamiętać, że urządzenia mobilne często mają w pamięci więcej wrażliwych informacji. SMS-y, MMS-y, kontakty, zdjęcia, filmy, ważne pliki, dane dostępu do kont, hasła do sieci i wiele innych. Dlatego warto zadbać o bezpieczeństwo, szyfrując nasze urządzenie.
W przypadku systemu Android jest to dosyć proste, ponieważ narzędzia potrzebne do zaszyfrowania całego urządzenia są już wbudowane w system i gotowe do użycia. Różnice zależą od wersji systemu zainstalowanego na naszym urządzeniu, a także od modelu smartfona, jednak nie powinno to stanowić problemu.
Uwaga! Przed rozpoczęciem procesu upewnijmy się, że nasze urządzenie jest naładowane, podłączmy je do ładowania. Pierwszy start po zaszyfrowaniu może być wolniejszy. Samo szyfrowanie urządzenia nie powinno negatywnie wpłynąć na jego osiągi.
Uwaga! W urządzeniach z Androidem w wersji 11 i wyższych cała pamięć urządzenia jest domyślnie szyfrowana – nie trzeba aktywować tej funkcji, nie da się jej również wyłączyć. Wskazówka dotyczy urządzeń, które pracują z wcześniejszymi wersjami systemu.

1 Przechodzimy do ustawień naszego urządzenia.

2 Naciskamy kategorię **Zabezpieczenia** **A** (lub jej odpowiednik).



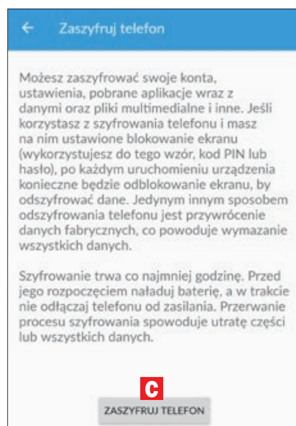
3 Naciskamy **Zaszyfruj telefon** **B** w polu **Szyfrowanie**.

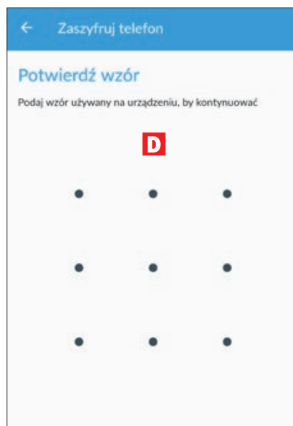


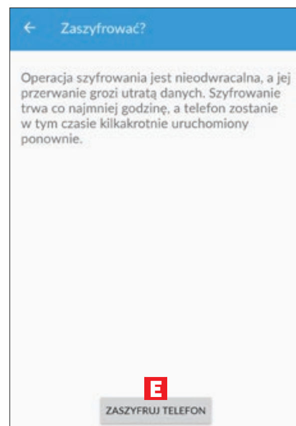
4 Teraz musimy zapoznać się z informacjami dotyczącymi szyfrowania. Jeśli wykonaliśmy wspomniane wcześniej kroki przygotowawcze, będzie dostępna opcja **ZASZYFRUJ TELEFON** **C**, którą wybieramy.

5 Teraz potwierdzamy wzór **D**, hasło lub inną metodę wybraną do zabezpieczania naszego urządzenia.

6 Przechodzimy do ostatniego ekranu, na którym wystarczy nacisnąć **ZASZYFRUJ TELEFON** **E**. **Uwaga!** Operacja jest nieodwracalna i po jej wykonaniu nasze dane zostaną bezpiecznie zaszyfrowane, a dostęp do urządzenia będziemy uzyskiwać każdorazowo po jego odblokowaniu za pomocą wzoru, hasła lub innej wybranej przez nas metody.







adam13zajac@gmail.com

JAK SKORZYSTAĆ Z E-WYDANIA KSIĄŻKI

W KŚ+ znajdziemy **e-wydanie tej Biblioteczki, obraz ISO dołączonej do niej płyty z najlepszymi narzędziami do ochrony prywatności w internecie oraz plik PDF książki do pobrania.**

1 Otwieramy stronę **ksplus.pl**. Logujemy się **A** (używamy konta z serwisu **Komputerswiat.pl**). Jeżeli nie mamy konta, klikamy na **B**, by się zarejestrować.

B Załóż konto Logowanie A
Zarejestruj kod

2 Po zalogowaniu się możemy zarejestrować kod nadrukowany na płycie dołączonej do książki. Wystarczy kliknąć na **C** i przepisać kod.

| Moje konto ▾
C Zarejestruj kod

3 Uzyskamy w ten sposób dostęp do e-wydania **D** i do bonusowego obrazu płyty **E**. Do serwisu KŚ+ możemy logować się z dowolnego urządzenia z dostępem do internetu.

CZYTAJ E-WYDANIE D
PROGRAMY E
BONUSY

UWAGA! W KŚ+ ZA DARMO E-WYDANIE KSIĄŻKI ORAZ PLIK ISO PŁYTY

POLECAMY INNE NASZE KSIĄŻKI



KURS PHOTOSHOPA

Photoshop krok po kroku, od podstaw do eksperta: najważniejsze narzędzia i najnowsze funkcje oraz wskazówki i przykłady, jak z nich korzystać. Na DVD: bank 1000 zdjęć i najlepsze programy graficzne.



JAK ZOSTAĆ TWÓRCĄ GIER

Programowanie gier w Unity i C# od podstaw – teoria i praktyka, własne projekty krok po kroku. Na DVD: najlepsze darmowe silniki gier, narzędzia dla programistów, pliki gier opisanych we wskazówkach.

Nasze książki w wersji drukowanej kupisz na literia.pl
Książki są również dostępne w formie e-wydań na ksplus.pl

adam13zajac@gmail.com



Krzysztof Dziedzic
autor książki,
informatyk

NIE DAJ SIĘ ŚLEDZIĆ!

Zachowanie prywatności podczas korzystania z internetu to jedno z największych wyzwań. Nikt z nas nie może i nie chce zniknąć z sieci – pracujemy zdalnie, utrzymujemy kontakty online i potrzebujemy internetu, by wiedzieć, co się dzieje, i mieć dostęp do informacji, no i wszyscy korzystamy z serwisów społecznościowych.

Czym innym jednak jest świadome dzielenie się z bliskimi i znajomymi wiadomościami, zdjęciami czy filmami oraz przesyłanie ważnych informacji do zaufanych odbiorców, a czym innym jest śledzenie i wykradanie nam naszych danych bez naszej wiedzy i zgody.

W tej książce przedstawiłem wiele programów i porad, które pomogą Wam zachować prywatność oraz anonimowość w sieci i kontrolę nad tym, jakie dane wydostają się z Waszego komputera i smartfona – to powinien być dla każdego z nas priorytet.

Wykorzystując opisane w książce programy, możemy zaszyfrować nasze dane i bezpiecznie komunikować się ze znajomymi bez ryzyka, że ktoś nas podsłuchuje.

Dowiemy się też, jak bronić się przed oprogramowaniem szpiegowskim typu Pegasus i jak sprawdzić, czy nasz sprzęt nie został zainfekowany. Duża część książki poświęcona jest ochronie smartfonów – ten temat jest często pomijany, a to właśnie ze smartfonów można się o nas najwięcej dowiedzieć.

Na płycie dołączonej do książki i w ksplus.pl znajdziemy komplet narzędzi do ochrony prywatności opisanych we wskazówkach.

CENA 16,90 ZŁ
W TYM 5% VAT

Płyta DVD jest dodatkiem do książki

ISBN 978-83-8250-139-1 INDEKS 321 958



Nr 2/2022 (118)



KOMPUTER
ŚWIAT
BIBLIOTECZKA